

The Kolkata

Vol 11 Issue 3 2022

Rs. 50/-



PROTECTOR

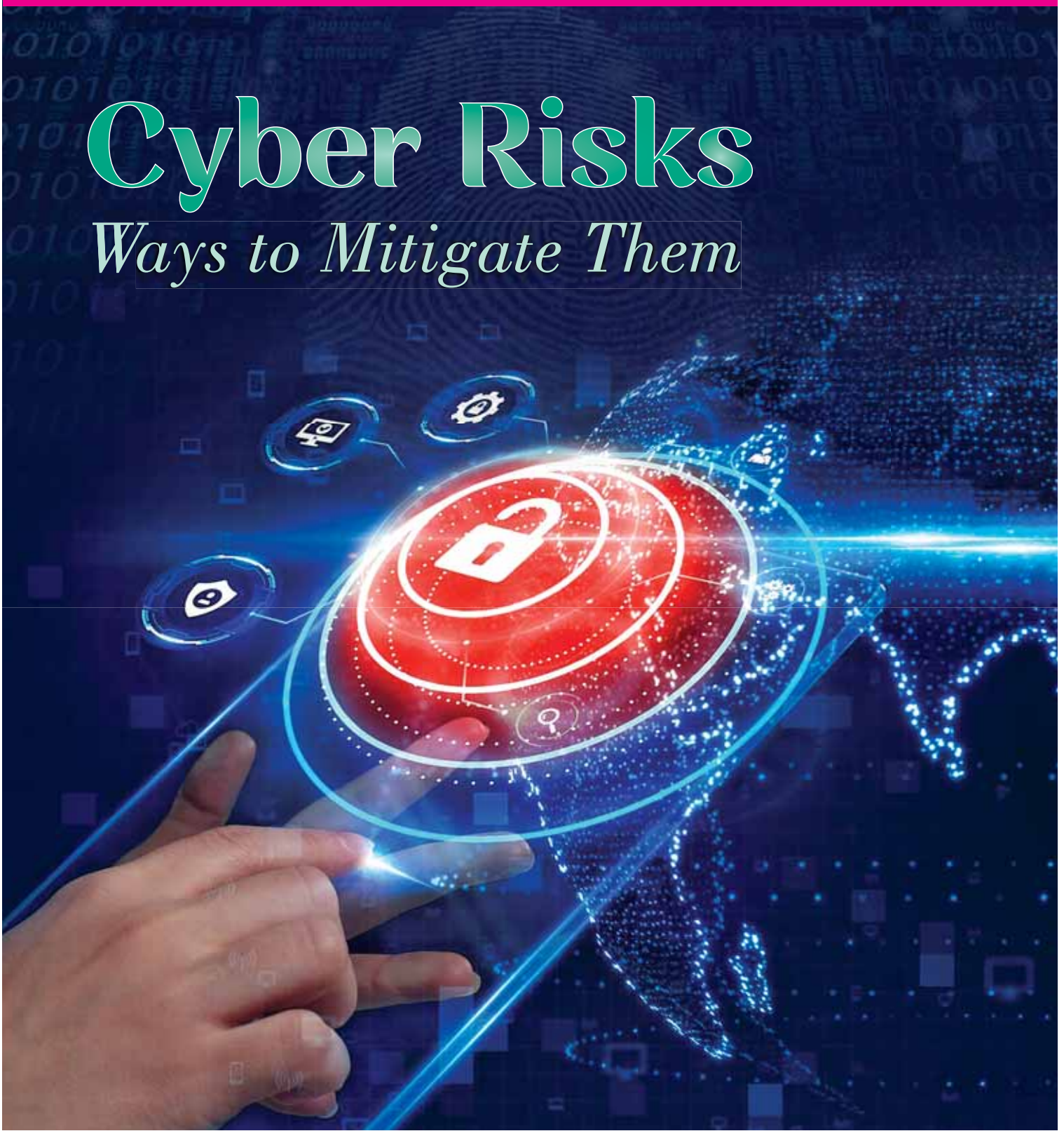
www.theprotector.in

A Magazine for the Kolkata Police

PROMOTING PEACE

Cyber Risks

Ways to Mitigate Them





KNOW ABOUT HEART FAILURE



**NARAYAN
MEMORIAL
HOSPITAL**
CARE CLOSE TO YOU



1) What is heart failure?

Heart failure is a condition in which the heart fails to effectively contract to pump out the blood around the body to maintain circulation for normal organ function. It may be due to damaged heart muscle or impaired relaxation of heart muscle.

2) Are heart attacks, heart failure the same?

No. Heart Attack usually due to blockage of the blood vessels supplying muscle to the heart and heart failure is the inability of the heart to pump blood to maintain circulation.

3) Why is it dangerous?

50% of heart failure patients die in 5 years time and large number of patients need hospitalisation due to worsening of symptoms. Sudden Cardiac death is responsible in 50% of mortality in these patients. Therefore intensive therapy at earliest very much imperative.

4) Common Causes of Heart Failure?

- Ischaemic Heart disease that includes previous heart attacks and atherosclerotic heart disease.
- Valvular heart disease
- Pericarditis, Myocarditis
- Congenital Heart Disease
- Rheumatic Heart Disease

5) Associated Conditions that may aggravate/increase the risk HF?

High Blood Pressure, Diabetes, Dyslipidemia, Chronic lung disease, Hyper/hypothyroidism, Obesity, Alcohol abuse, Drug intoxication,

6) Is it a Disease of Older population?

Heart Failure can affect all age groups. It is not confined to older people only. Although the risk increases with increasing age, young people can also suffer from heart failure if they have pre-existing heart disease. As per Data Indians develop heart disease 5-10 years earlier compared to other ethnic populations.

7) What are the sign and symptoms of Heart Failure?

Breathlessness on minimal exertion, on lying flat, bending down or leaning forward, Swollen ankles, legs, Excessive fatigue, Nocturnal cough, Chest pain or pain in the abdomen, Puffy face, excessive Sweating with cold extremities

8) How can it be prevented?

No to sedentary lifestyle. Engage in physical activity like Walking, Jogging, bicycling, Regular Exercise. Avoiding excess salt, Refrain from the consumption of processed foods and fast foods, Maintain a healthy weight. Monitor blood pressure regularly.

9) How is heart failure diagnosed?

Clinical profile, Basic Blood tests including biomarkers like NT pro BNP, ECG, and Imaging Modalities like Echocardiogram.

10) Treatment of heart failure?

Standardised guidelines based Medical Treatment that combines lifestyle modifications, Regular medications, check ups and routine follow ups with specialist doctor is needed.

Along with that treatment of comorbid conditions is also essential to prevent complications.

Medications: Four pillars of Drug regimen are now established in treatment of Heart Failure with Reduced Ejection Fraction patients. That Includes ARNI, Beta Blockers, MRA

(Mineralocorticoid Receptor Antagonists and SGLT 2 inhibitors. Apart from That Diuretics are needed to control symptoms of congestion. Patient may also need blood thinner, antihypertensive, antidiabetics depending upon underlying condition.

Devices: Along with optimised medications this patients are need of certain device based therapy to prevent sudden cardiac death and to improve symptoms.

ICD: ICD devices are implanted to prevent sudden cardiac death in heart failure patients.

Here One Such device is implanted in left side of chest and two wires which are connected to the device goes inside heart chambers. Whenever any arrhythmic activities are noted the device delivers shock to prevent SCD. There should not be any fear from such shock as this is life saving and devices are programmed with advanced algorithms to control such arrhythmic episode without even shock.

CRT: CRT devices are one of very important therapy in heart failure patients where three wires are passed to heart chambers and the connected machine is implanted over the left side of chest wall. It basically synchronises between two ventricles in terms of contraction and optimize the outcomes. A large number of patients experience improvement in the LVEF post implant of CRT devices and therefore become devoid of such symptoms of Heart Failure.

CRT devices are more often combined with ICD as called CRT-D to give the dual benefits of improvement of LVEF as well as prevention of SCD. Apart from that patient may require mechanical support like IABP and several LVAD devices as bridging therapy to failing heart. In that scenarios the ultimate definitive therapy is Heart Transplantation.







DIGITAL VIGIL

Next Level Policing

Policing is always an ever-evolving subject. The never-ending spree to remain vigilant offline and online is the hallmark of modern-day policing. An IIT grad at the helm of Kolkata Police has rightly reinforced the digital domain of the department which has always been ahead of other police forces around the world. Under the guidance and able leadership of new Commissioner of Police Vineet Kumar Goyal, the policemen are now ready for the next level challenge – protecting the city and the netizens against cyber criminals across all levels and layers of security.

All over the world, the digital shift is prominent in the crime pattern. The lockdown phase was an eye-opener. Traditional culprits deviated from their conventional modus operandi. The digital domain is relatively unprotected as

no physical jurisdiction is applicable. Not only that, social media like Facebook, Twitter, Instagram, and WhatsApp, which have become indirect hubs for a data breach or data sharing by unauthorised cyber personnel, are owned by corporates belonging to other countries. This has necessarily demanded a change in the entire approach. But along with the police, there are key stakeholders in the digital world, who can cater to better cyberspace. The industry stalwarts who are innovating with modern technologies can make the virtual place safer and digitally healthier. The recently concluded Bengal Global Business Summit (BGBS) has shown that Bengal has all the capabilities and promise of becoming the next destination for all digital enterprises. A wholehearted approach from the corporate world, ethical hackers, experts, and researchers is always welcome.

Presently, all the police stations of Kolkata Police have trained cyber police personnel who are ready to help. Upskilling of the police officers, top to bottom, has been an excellent ongoing practice in the Kolkata Police force. Whether it is an economic loss to victims or damage to social profiles or a bigger threat - the Kolkata Police force has an inclusive viewpoint and work action plan to solve various issues including internet fraud in the best interests of the victim and society at large. Added to that, the Kolkata Police is educating the masses, focussing on mass awareness and precautionary measures, to avoid mistakes on the individual front. One of the most common features of cybercrime has always been the lack of awareness of netizens. Any particular digital activity which may seem to be normal can make an individual susceptible to a data breach or victim of digital fraud.

As of now, the Kolkata Police have solved some critical cases concerning internet fraud. Added to that, the department has received accolades for some path-breaking innovations in decoding cybercrime rackets. From a community perspective, there has been a special focus on safeguarding senior citizens who are naturally most vulnerable to the internet and cyber fraud. Almost all police stations are working in tandem, initiating WhatsApp groups, door to door campaigns on what to do and what not to do. Already, many cases have been avoided as people have complained regarding any suspicious call or message, impersonating some other person or organisation.

But the battle is not over. Whether it is business email compromise, criminal cooperation across various levels, distributed denial of service attacks, modular malware, non-cash fraud, online child abuse or ransomware, SIM swapping, smishing attacks, or phishing – there is a sense of urgency when it comes to new technology associated with cybercrime. The fact remains that reporting cybercrime helps police to crack lots of cases. The more victims report a crime, the more data the police can gather and establish connections between cases, and it becomes much easier to tackle the most modern mode of crime.

The efficiency, dedication and commitment on part of the Kolkata Police is unparalleled. We hope the Kolkata Police will continue to work with the same zeal online, making netizens of the city safe and secure in the days to come. After all, there is nothing so protective and assuring than the ever-vigilant Kolkata Police.

A handwritten signature in blue ink, appearing to read 'Satya Swaroop'.

Satya Swaroop

Managing Editor

satya@newmediacomm.biz

 **Executive**[®]



Furniture



ANANYA

BONHOOGHLY

SODEPUR

UTTARPARA

SERAMPORE



Kolkata Police has always been marching ahead with a modern outlook on policing, with an urge to serve the people with care, concern and commitment. In the last two years, ever since the lockdown phase, the police force has reached out to the masses with a more social perspective, in the greater interest of the city. I congratulate the entire police force for their exemplary dedication and wholehearted approach.

In terms of traditional crime committed, it is quite evident that there has been a gradual shift in it. Cases of snatching, theft, robbery, burglary, homicide, abduction, trafficking etc. are seeing downward trend in last few years in Kolkata. The general awareness, local administration and peace-loving nature of the people have been pivotal in this regard. But complaints of bank fraud, email scams, password hack, identity hacking in social media are seeing upward trend. We are moving towards zero tolerance against cybercrime with renewed vigil and concern.

The purpose of technology is to make our lives easier and better. But technology has also indirectly enabled individuals to commit crimes right from their homes or workstations by using electronic devices under anonymity. Technology has changed the pattern of crime. The evolution of cybercrime in cyberspace has witnessed various types of online criminal acts including identity theft, ATM or credit card fraud, online sexual harassment or blackmailing, cyber-bullying, inciting violence through fake social media posts and various other modes. In the case of social media, the biggest mistake has been the case of oversharing of information and data. Netizens share much more personal information online in the public domain. This makes the netizens vulnerable to cybercrime. No doubt, individuals who are very active in social media, are at greater risk of being targeted. Sharing detailed information with strangers is also a major concern. In the case of bank frauds and email scams, often cybercriminals opt for social engineering methods to get various types of private data and information of the victim.

Cyber policing has been the new addition to police forces around the world. In Kolkata, there has been a constant upgradation with regard to enabling the officers of Kolkata Police to tackle the cybercrime complaints with equal commitment and care. There has been a constant technical know-how exchange with the IT industry to respond to variety of crimes committed in Cyber Space. Based on the level of impact, deployment of the police force is needed in the cyber domain. Based on the threat level, there can be large scale, medium scale and small scale cybercrime incidents. In case of large scale cyber incidents, a nationally coordinated response is required where the police and the national law enforcement agencies work in close coordination. On a medium scale, cases of data theft are trending in the corporate segment. As of now, the police stations mostly have to deal with the small-scale incidents of cybercrime. There is no denying the fact that the susceptibility or vulnerability of the netizens can be reduced to a considerable extent if there is awareness at the grass-root level.

The Kolkata Police force already has a team of cyber experts and all the divisions presently have the digital expertise to tackle such issues with care and concern. Through the social media and various other modes of public interest, the Kolkata Police is constantly engaged in disseminating the do's and don'ts for everyone in the digital world. The Pranam teams are also working in tandem for the digital safeguarding of the senior citizens who are extremely vulnerable to cybercrime.

Kolkata Police is known for its efficiency in detection of crime and exemplary punishment for the perpetrators of crime as per the law of the land. I am certain that Kolkata Police will constantly upgrade to emerging challenges posed by latest trends in cybercrime and meet the expectations of the people.



Vineet Kumar Goyal IPS
Commissioner of Police
Kolkata



PARADIGM SHIFT IN POLICING

In an exclusive interview to Anurag Sinha, Regional Head, New Media Communication Pvt Ltd, the Commissioner of Kolkata Police, Vineet Kumar Goyal, shares the ongoing details of the technological upgradation of police force and measures taken to check the cyber crimes in the city

Q: Technological upgradation has been the key to most police forces around the world to tackle crime and provide better services. What aspects on

the technical front are on your agenda as of now, especially the short-term and long-term ones?

A: Technological upgradation has always been the key to modernising the police force. With changing times, there have been technological advancements and the need of the hour is to keep up with these advancements to provide better services to citizens.

The pattern of crime has changed over the years from conventional crimes to hi-tech crimes such as identity theft, phishing, vishing, hacking, cyber stalking, cyber terrorism, ransomware & malware, etc. Growing incidents of cyber crime has become a challenge for the force. Kolkata Police has taken up the challenge to eradicate

these new age crimes. We have launched extensive awareness campaigns through which citizens are being sensitised on the etiquettes that need to be followed while using digital platforms for making payments. That OTPs and passwords should not be shared with any unknown persons. As a means of enforcement, we have created cyber labs in each of the nine divisions where specially-trained personnel are posted for detection of cybercrimes. These labs work 24 X 7 and attend to reports of cybercrimes immediately.

We are reaching out to citizens through different e-platforms to ensure that they get the requisite services without delay. As an example, I may cite the instances of obtaining Police Clearance



Certificate, Arms Licence, Post Mortem Report, payment of traffic fines etc. that are available online through Kolkata Police website and also through Bondhu App.

Another important aspect would be to enhance overall travel experience across the city and reduce the travel time of commuters without compromising on the safety of the commuters.

Q: Do you think there has been a paradigm shift in the pattern of crime committed in the digital world? Is it due to the impact of the COVID-19 pandemic?

A: It has been observed lately that there has indeed been a paradigm shift in the pattern of crime committed. The digital world is

the most affected. People who are extremely active in the cyber world have been victims of cyber criminals. Cyber-crimes are becoming more and more sophisticated and the criminals are continuously changing their modus-operandi by exploiting technological loopholes or social engineering techniques. Many people, who are not well acquainted with technological advancements, are the easy prey to these prowlers.

As more and more people started using digital wallets, the cyber criminals started picking these pockets and thus came into being the cyber pick-pockets – if we may call them so.

The pace of digitisation went up significantly during COVID times, therefore, vulnerability of

citizens to cyber criminals has also increased.

However, those who exercise due care and take adequate precautions while venturing into the digital world, are seldom affected.

I would request all readers to never share OTP/ Bank Account Number/ Credit/Debit card details and other personal information with anybody.

It is our motto to make all aware and keep on telling them to exercise due care and precaution while accessing the digital world. Kolkata Police has set up Cyber Labs in every division where technically trained police personnel are posted at every police station to aid and assist victims and also help in the process of investigation.



Q: Over the years, Kolkata Police has given massive importance to community level policing. What steps the management is thinking to take it to the next level and bridge the gap?

A: Kolkata Police is a citizen-centric police force. There are several community policing initiatives that cater to every section of society. Initiatives such as Nabadisha provides free education to street children, Pronamaims at interacting with the senior citizens and attends to their needs and necessities, Tejashwini aims at imparting training in self-defense to girls of different ages, Goalz, para football & school footers aim at building a bridge between the community and police through a popular game of football, Kiran provides computer literacy to the poor and the needy. So, the community works as the eyes and ears for the police. It is the residents of a community who help police in performing their

work with ease and efficiency. If the residents do not give proper information to the police about the goings-on within the locality, it will be extremely difficult for police to curb the crime.

Police have always been working hand-in-hand with the community and have always been interacting with the community to boost policing.

Q: Police are supposed to be friends and not to be afraid of. Still at the grassroots level, many people look reluctant to report crimes. What may be the possible reasons for such reluctance?

I beg to differ with you here. This perception has been changing over the years. Kolkata Police has taken up several outreach initiatives that allow us to reach out to the community and interact with them more often and in a friendlier way.

Q: Would you like to add new initiatives taken by

Kolkata Police under your leadership?

My focus will be on public outreach and technological interventions:

- i. Effective management of law & order in the city
- ii. Crime control with special focus on cyber crime
- iii. Dial 100 system is being revamped to ensure quick response to public complaints. Response time has significantly reduced.
- iv. Reduce travel time & improve travel experience
- v. Reduce road traffic accidents without compromising on travel experience

For public outreach, all police stations have been provided with a dedicated mobile number and handset where people can lodge their missing diaries without going to the PS. This system was found to be extremely useful during the COVID times.

Police stations have also taken the initiative to regularly interact with all the senior citizens in the area as part of the Pronam initiative. Officers from the PS have used video conferencing platforms to enquire about the well-being of senior citizens and provide them with their needs and necessities.

Automated synchronized signalling system is implemented using PLC connected with the central command and control centre using fiber optics with signal optimisation.

We are also working with Google to use Google Live Traffic data to predict congestion, to optimise phase times of these signals in real time that is likely to further enhance the travel experience and reduce congestion.

We are also working on Parking Solutions for the city. This will enhance the parking system in the city by making parking slots available to all on a real time basis. The data obtained is also likely to be useful for future policy making.

Q: In your long illustrious career, what has been your secret to success working across various high-profile assignments?

The blessings of my parents, grace of God and hard work throughout my career have been secrets of my success. I have been extremely fortunate to have found a team who have been extremely efficient and helped me in achieving many daunting tasks.

Q: If possible, share some details about the famous encounter in New Town in the year 2021?

On 09.06.2021, on the basis of information, a team comprising of Special Task Force, West Bengal, with the help of specially trained men, led by myself along with IG STF, raided Sukhobristi Apartment, New Town where two dreaded gangsters from Punjab were reported to be hiding. This housing complex is home to more than 10,000 families. The prime objective was to arrest the wanted gangsters. Accordingly, the teams were briefed to follow Standard Operating Procedures and were deployed to prevent escape of the wanted persons. With such a heavy density of civilian population, extreme caution had to be exercised to safeguard the civilian population.

These gangsters were reported to be extremely desperate and had killed two on duty ASI of Punjab Police. They had also committed several heinous crimes like murder, dacoity, kidnapping for ransom, looting of arms of police personnel etc.

When our arresting party entered the flat, a scuffle took place. One of our officers from STF WB was able to apprehend one of the gangsters but suddenly the other gangster opened fire on the police team. One bullet hit the officer and he was seriously injured. Taking advantage of this, the other gangster also took out his weapon and started firing on the police party.

STF team responded with due courage and showing presence of mind evacuated the injured officer and in self-defence engaged the gangsters in retaliatory fire where both the accused persons succumbed to the bullet injuries sustained by them.

After the incident, the investigating agency found a large cache of arms and ammunition, several sophisticated arms, huge quantities of live ammunition, Laptop & Printer, mobile phones, huge amounts of cash and other articles.

The STF WB team showed exemplary courage and completed the entire operation without any harm to the civilian population. •

GLUCONATE HEALTH LIMITED
(A Government of West Bengal Undertaking)
HO/RO : 2 Durga Charan Doctor Lane, Kolkata- 700 014
Tel : (033) 2265-0001 (3 lines FAX : (033) 2265-8537
E mail : ghldm@rediffmail.com

Manufacturer of :-

- ALKACITRON
- SIMPCLOX
- VALOL
- AZINET TABS 250 MG/500 MG
- BRUGESIC P
- AMOXYCILLIN TRIHYDRATE CAPSULE
- NORFLOXACIN 400 MG TABS
- METRONIDAZOLE TAB 400 MG
- PARACETAMOL SUSPENSION
- METRONIDAZOLE SUSPENSION

Factory :
1 Health Institute Road, Kolkata – 700 065
Dum Dum Cantonment
Tel : (033) 2566-2075/3220/5479/2283

Subhankar Sinha Sarkar, IPS, Jt. CP Headquarters, shares his thoughts on a number of issues, including community policing, cybercrimes, and difficult phase of Covid pandemic, and how the Kolkata Police managed them with great care, getting admiration from the masses.

FAILURES TEACH YOU TO BECOME STRONGER

A decorated officer with exemplary dedication and commitment to work, you have been a brand on your own for youngsters in the force. What has been the secret for your success in uniform?

Since my journey started in the field of policing, I have learned a lot from my failures rather than my successes. However, what I always tried to carry within myself is my positivity towards work. It is always very encouraging

and satisfactory if my dedication inspires my team members.

To me, "Success and failure" are two sides of a coin. I have always believed in a very basic notion i.e. "Happiness is the key to success and if you love what you are doing, you'll surely be successful". I think that success is nothing but a series of experiences of having failed at

times and no one can be successful in every sphere of life. Failures teach you to be stronger. However, to be successful in this prestigious profession, one should have the traits of self-belief, patience, discipline, dedication, innovation, presence of mind, team work, leadership and most importantly to be happy with one's work.



The pattern of crime in India has already witnessed a major change and Kolkata is no exception to that. How is the Kolkata Police looking at it with a renewed approach?

New age brings new problems and to solve those tribulations, the police need to be more and more advanced in every sphere and the Kolkata Police is no exception. A good thing about the Kolkata Police is that it always tries to innovate and learn.

A surge in phishing attacks, financial frauds, spam mails and ransomware attacks were reported during the Covid-19 lockdown period, when people mostly worked from home and attackers impersonated brands and misled employees and customers.

To counter the new age cyber-criminals, more training programmes, crisis management plan for countering cyber attacks and cyber terrorism, conducting cyber security mock drills and exercises to enable assessment of cyber security posture are needed.

One awareness programme, widely known as 'Raksha Kavach', launched by Kolkata Police, aims to teach citizens how to protect themselves from cyber criminals. The Raksha Kavach programme has already reached every nook and corner and it has been instrumental in ensuring that residents report even unsuccessful attempts of cyber crooks. Our main concern naturally lies with the elderly as they are the soft targets of cyber attacks. Kolkata Police has been conducting general awareness programmes regarding these new threats at every possible place. A dedicated mobile no. 9836513000 of Cyber Police Station has been working 24x7 to register

any grievances related to cyber crime. Moreover we are very active on social media warning people every day about these threats.

To conclude I must say that the Kolkata Police is always prepared to counteract any type of crime in society.

Almost in all countries, officers in uniform have faced immense stress in the COVID-19, watching deaths of their colleagues, friends, family members while working on the frontline. What is the best way to handle stress in such circumstances?

To opine that there is no such shortcut to handle stress, but we have to curtail its rampage and we usually do it successfully.

Being uniformed, it was our duty to implement Government guidelines whatever be the matter. We have been trained in that way. As we were doing only duty in such calamity, there was no option to get stressed, there was only professionalism. We have seen the tumultuous outbreak of Covid-19 within our force, family and friends and witnessed fatalities in the line of duty. Its increasing dominance tore our mental serenity apart but our professional fraternity has trained us in such a versatile way to handle these types of wretched situations with subtle hands. These dreadful circumstances made us even stronger than ever. We've started motivating our forces to concentrate on themselves regarding the maintenance of Covid protocols, add in better food habits, proper sanitizations in their daily routine. Thus the modus-operandi helped our police force immensely to handle stress.

There has been a major shift in crime in Indian society, cybercrime being the new entrant. Do you think policing in India needs an overall digital facelift to handle this emerging trend in criminal offences?

We all know that cybercrime brings a new era of challenges nowadays. The over-dependency on the digital platforms particularly in COVID times has paved the path for the cyber-criminals to implement their ulterior motives. This new phenomenon of cyber threat has a lot of varieties like financial threats by compromising passwords, cyber bullying, cyber stalking etc. As these cyber-criminals have no geographical fencing, the policing in Kolkata as well as in the whole country has already undergone a digital facelift to bring such criminals before the law. From the police station level, district level, state level and finally to the national level, everywhere the police forces are well equipped, well experienced, skilled, and specialized units to stop cybercrimes and cyber threats with ultimate potential. These cyber-criminals are the threats not only to an individual but also to national security. Therefore, to deal with all the odds created by such criminals, the police force has to be more proficient and every aspect of that has been ensured. Recently, the Kolkata Police set up Cybercrime investigation labs in each of its divisions and the state forensic laboratory has created specialized posts for digital forensic evidence recovery. Moreover, a special anti-stalking helpline is operational.

A dynamic force like Kolkata Police has always risen up to the mark to defend every citizen with ultimate



support from every corner of society.

In most countries, community policing is considered to be the vital link of policing. What according to you is the most important aspect in this regard for Kolkata Police?

Community policing is truly one of the most vital links to governance in policing nowadays. Like most of the renowned police forces all over the World, Kolkata Police incorporated this method to form a strong social order. The Kolkata Police fraternity has formed several community policing initiatives like Pronam, Kiran, Nabadisha, Sukanya, Tejaswini to strengthen the bond between civilians and police force. During Covid-19 pandemic, the Kolkata Police went beyond the regular policing and stood by the civil society like the pillar of strength and served food and medicines to the people, created awareness among citizens to keep

the disease at the bay, protected the citizens from the pandemic as far as possible alongside controlling crime and maintaining law and order, bringing essentials to the senior citizens as well as to every humdrum in need during lockdown. This is definitely a very crucial way to penetrate into the heart of society that sincerely motivates the morale of citizens which not only enhances the public relations but also reduces the rate of crime.

As the corporate sector has witnessed a downturn and job losses, many Indians are focusing on government jobs. What should be the ideal approach for a civil servant aspirant while studying from home with limited resources?

It is a basic topic in most of the middle class families who want their child to get into a government job, not in a private one and these

days this thought has ample reasons in its support. Due to the Covid pandemic, a lot of corporate or non-governmental sectors fired their employees or curtailed a good percentage of money from their salary. Though this lacuna might be sorted out as soon as the effect of the pandemic is over, still these types of insecurities have been making the youth focus on more secured Govt. jobs. However, the Indian government job, especially the civil service, is one of those elite jobs which everyone aspires to. Anybody who wants to pursue a career in civil services must be aware of his/her surroundings and should have an analytical approach. Firstly, the aspirants should properly go through the syllabus of the civil service exam, then specifically work on the current affairs, Governmental policies, political fundamentals, scientific innovations, India and its relations with other countries, Indian Constitution, Indian History, national struggle, moreover the world at large. Everything can be

easily followed from home using digital platforms. He/she can easily get anything regarding their need in the digital web as there is no dearth of resources over there. Moreover, in the Govt. scheme named Digital Library India, all kinds of books or resources are available free of cost. Aspirants should make good use of these from their home, besides, they have to develop the quality to analyze the subjects from different perspectives and form opinions.

It is often said that representation of women in the Indian police fraternity is still not up to the mark. The same is often said about the Indian armed forces. What should be the approach to encourage more women to join the forces? Is gender sensitization much needed at the grassroots level?

First of all, I must point my finger at our basic age-old propaganda of family policies regarding women which has to be corrected. Our patriarchal mindset towards women has to be altered. This is nowadays a major subject of concern resulting in debates amongst civil society as well as Government policy makers. In comparison with the initial days when the uniformed services used to be male dominating, nowadays the situation is gradually improving not only in the subordinate ranks but also in the supervisory levels and women personnel have been performing so well, at times better than their male counterparts.

Although, there are still a lot of shortcomings for them like, shortage of decent accommodation, separate washrooms, changing rooms etc. However, these infrastructures are being updated gradually.



Moreover, the outlook of society and families are also changing. Now, we can find a good number of lady police personnel in most of the units and they have been doing so well. Gradually, the increasing intake of women personnel will decrease the imbalance in the force itself and it will also be better for society to get security for women from the women which will definitely encourage more females to get into forces.

The Covid pandemic presented a unique approach to policemen and women, demanding a 360 degree application in community policing. Is it the time to say that community policing is the most futuristic and inclusive mode of modern day policing?

Like we all know that the Covid-19 pandemic is one of the reasons that our police department has come a bit closer to the communities in their time of needs during lockdown but the ventures which Kolkata Police has already started long before this pandemic under the Community Policing Wing are truly very

humanitarian and effective in all regards.

Basically Community Policing emphasises proactive problem solving in a systematic and routine fashion. Rather than responding to crime only after it occurs, community policing encourages agencies to proactively develop solutions to the immediate underlying conditions contributing to public safety problems. It is a law enforcement philosophy that allows police to continuously operate in the same area in order to create a stronger bond with the citizens living and working in that area. Community policing is defined as involving three key components: positive interaction, partnerships and problem solving.

Whereas, the traditional policing is very reactive in nature and crime fighting focused, the community-operated policing is more effective and proactive and works with the community to solve "problems" that have the potential to become crime. It involves anyone collaborating with the police to identify problems within the areas they live. As a result of which, the crime rate has been gradually decreasing and it is proving its worth as the most futuristic and inclusive mode of modern day policing. •



Finding Solutions for the City's Traffic Snarls

IPS officer **Atul V**, Deputy Commissioner of Police (South), Traffic Department, talks to Ranabir Bhattacharyya of Team Protector, on various issues including traffic problems of the city.

From a journalist in one of the most popular publications of the country to a decorated IPS officer, what is your take on this amazing journey? Has there been any change of perception on policing as a whole?

During my time working as a journalist, the focus was always on what is bad and ineffective in our society. As they say, good news is no news. This was despite the fact that the publication I worked for tried its best to highlight positive stories. But I always wondered, why are things so bad? Are they really so bad? This prompted me to try and work for the government, to find out on my own how and why things work as they do in the complicated system of governance. After almost nine years as an IPS officer, I am only a little wiser than I was before, but certainly a lot less judgmental than I used to be. Regarding policing, I can say that my perception as a layman was obviously very different from now. Today, I intimately know and face many difficulties that policing in India entails.

It is often said that distorted urbanisation, population, increase in number of vehicles are the main reasons behind traffic problems in metro cities. What attributes do you want to point out more in Kolkata's own traffic problems, especially in the added area?

Kolkata is also witnessing the "urban sprawl", a phenomenon seen all over the world and one of the main characteristics of this is the use of private vehicles for transportation. The stakeholders in the smooth running of traffic in a city are manifold. Sustained effort



to promote a culture of reliance on public modes of transportation will yield the desired result over a period of time.

From shopping malls, schools, colleges, universities to healthcare centres - there is always heavy traffic in the peak hours. What are your plans to cater to seamless traffic in the area?

Besides proper maintenance of road surface and street furniture in coordination with civic agencies, Kolkata Police is also constantly trying to introduce evidence-based technological interventions to reduce travel time for commuters, especially during peak hours.

This part of the city boasts of many high rises, and there have been cases of drunk driving and speeding as well. Which components are you looking to include to scale up the night traffic in the best interests of the city?

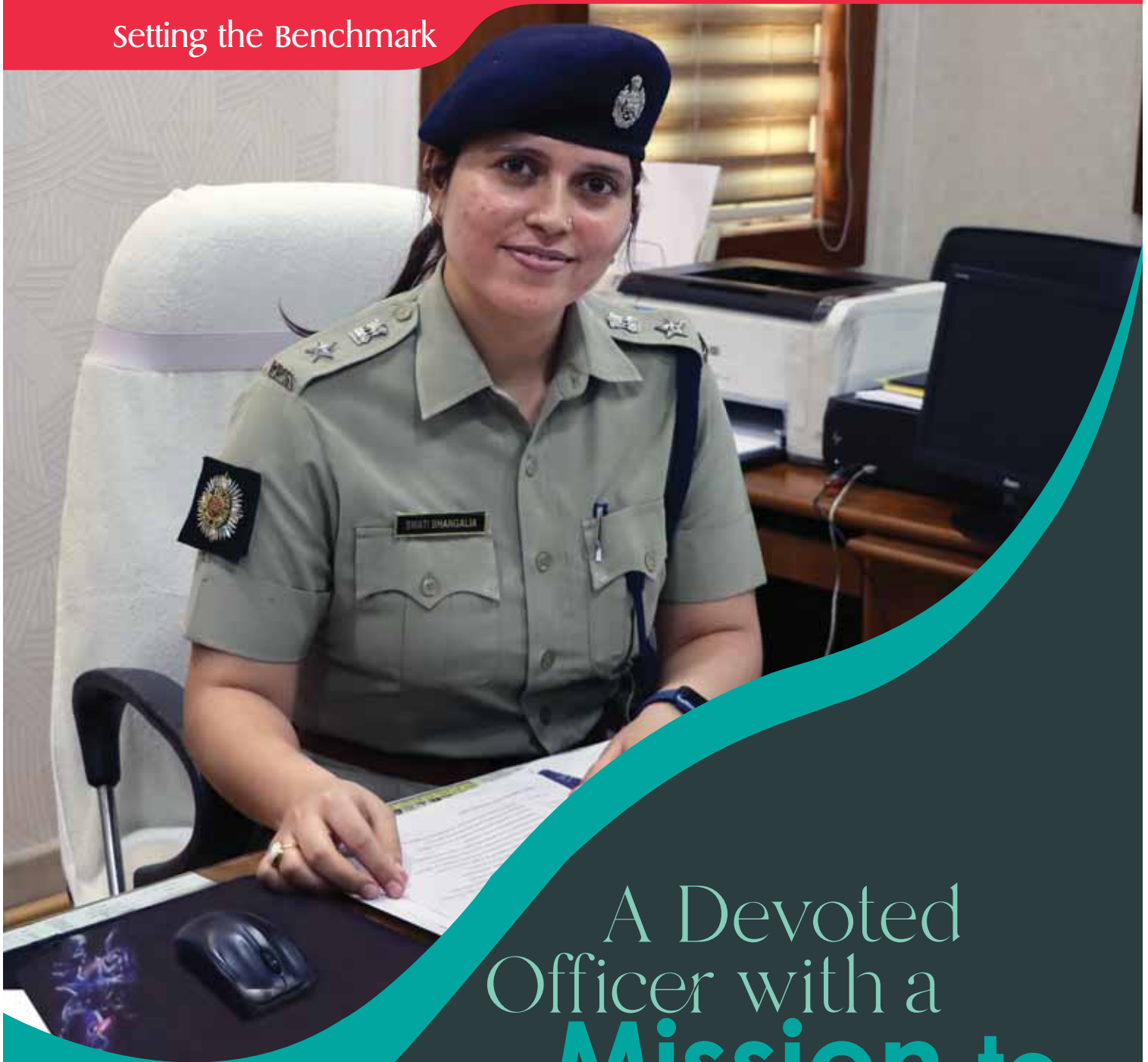
Regular raids and naka checking are held during the evening and night hours to curb drunk and dangerous driving. We try to keep moving the checking points, allowing for an element of unpredictability during special drives.

In various parts of the Greater South Kolkata area, there are narrow alleys and roads. What is your take on improving the parking issue? Do you think any innovation can ultimately help ease the issue and improve road traffic?

Parking space for vehicles is a complicated matter with many issues that need to be addressed in consultation with the municipal corporation. The problems and their solutions have a local element and are, therefore, managed at that level.

Being an avid traveller who has stayed in almost all the metro cities at some part or the other in different capacities, what finer aspects do you see in policing in Kolkata?

Even though I have stayed in many cities, it is only in Kolkata that I have been a policeman. Policing here has its own set of special challenges. My experience so far has been that these challenges are faced with utmost professionalism by police officers of all ranks here. Every member of Kolkata Police is extremely proud of this organisation and tries his or her best to discharge the given functions with utmost sincerity. •



A Devoted Officer with a Mission to Succeed

Swati Bhangalia, Deputy Commissioner, South - West Division (Behala) of Kolkata Police, tells Ranabir Bhattacharyya, about her civil service journey and steps taken to curb cybercrime in the city.

A B.Tech in Biotechnology and having an MBA in her kitty, Swati Bhangalia has been an exceptional student since her childhood days. Born and brought up in Delhi and having roots in Himachal Pradesh, excelling in academics has always

been a priority for her.

After completing her MBA, she decided to join her family business to help her ailing father. But the world of business didn't meet her expectations.

In her own words, "I was missing something in our day-to-day business activities. My father always wanted me to join the civil services. At that juncture, I planned to give my best effort. There was a complete change to the whole perspective, but a fighter as always, I was ready to accept the challenge."

Civil Service Examination – Grit, Determination and Patience

Her first attempt at the UPSC Civil Services examination was merely a dress rehearsal or rather pitch testing, as Swati didn't get time for preparation. But it ignited her inner spirit and thereafter, there was no looking back. Rigorous preparation from a reputed institution in Delhi did help her out with a concrete systematic approach, Swati prepared hard with the right strategy. Interestingly, she was keen to join the Indian Foreign Services but destiny had other plans.

"When the results came out, one of my friends called me up. I had never seen my father so happy in his life. Joining the Indian Police Service (IPS) was a tricky call at that time, but presently, when I look back, I am so happy to have taken the decision at that time," added IPS Swati Bhangalia.

Journey in Uniform - A Brand New Chapter

Initially, IPS Swati Bhangalia was posted in the Sikkim cadre, but later she took transfer and came to Bengal. In her own words, "My connection to the Bengalis goes back to my days in Delhi. I remember, every year I used to visit the Durga Puja celebration in the CR Colony. When I came to Bengal, I was ready for the task ahead. I was posted as the ACP in North Howrah in

2016. I was so fortunate that I was chosen to be a part of the team to give the Guard of Honour to our Hon'ble Chief Minister, Madam Mamata Banerjee. Thereafter, I worked in Kalyani as Additional SP and later in Chandannagar as an Additional DCP, working in the DD Department." During her days as DC South of Howrah Police, IPS Swati Bhangalia showed immense expertise, courage and conviction in her abilities in various capacities. In fact, on one such occasion, she got seriously injured but got back soon to the duty, standing by the force she had worked with. Presently, IPS Swati Bhangalia is posted as the Deputy Commissioner, South - West Division (Behala) of Kolkata Police.

Digital Stride - Tackling Cybercrime

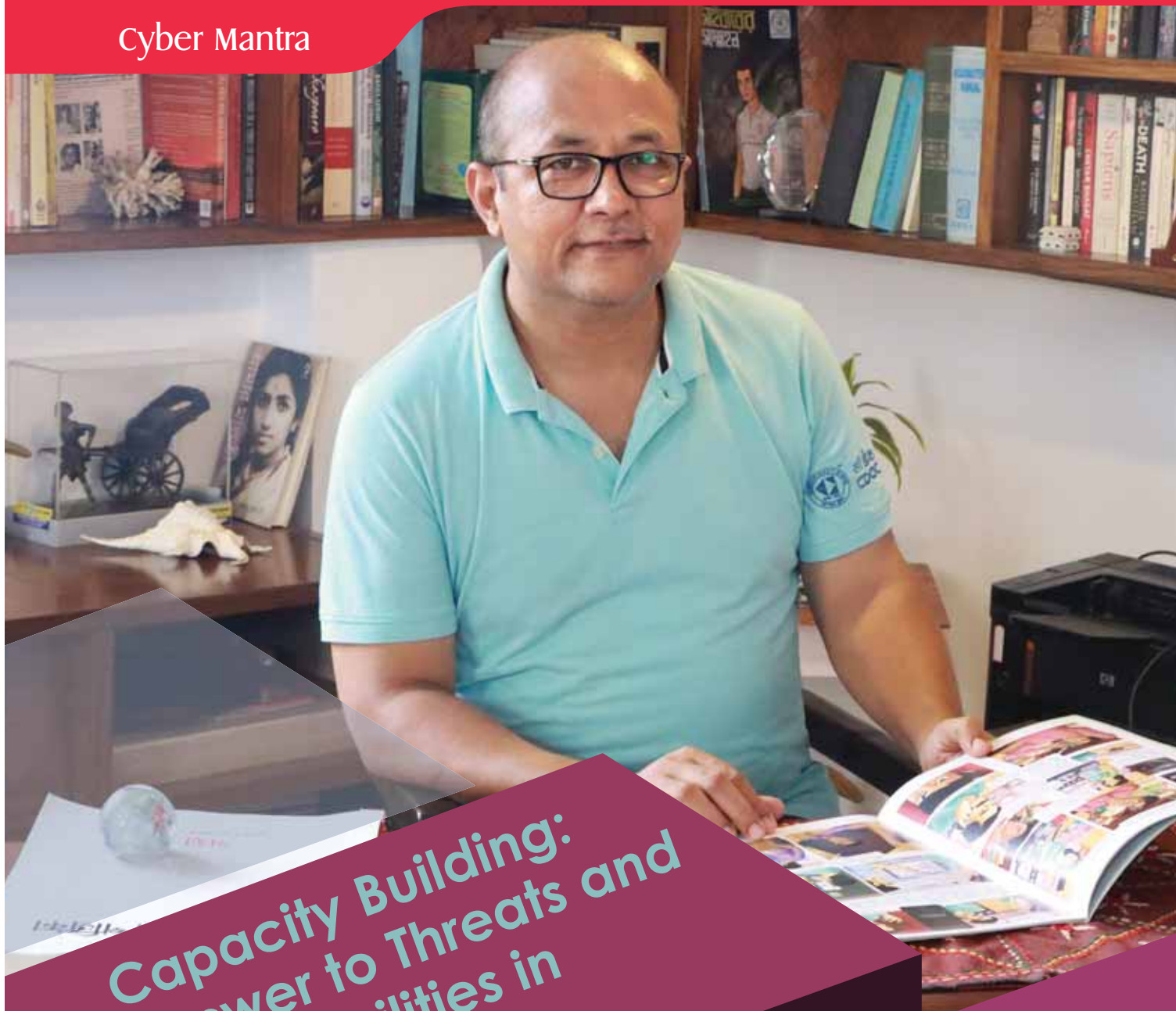
Ever since IPS Swati Bhangalia took charge of the South-West Division of Kolkata Police, there has been a sprint in the local police force's onslaught against the cases of cybercrime. Coordination with all the stakeholders has been the key, to provide a single-window solution to the victims. Added to that, various portals have been launched already under the Kolkata Police. "The portals provide the live status of the cases. Whether it is a case of bank fraud or troll or digital defamation, we have received a good response from the netizens. Not only that, we are encouraging people to report complaints to the nearest Cyber Cell of the Kolkata Police. Many such cases of extortion or blackmailing can be handled with due care if netizens complain in the beginning," added IPS Swati Bhangalia. In a recent case, where a guy hailing from Howrah came up with a Facebook post, falsely claiming a communal angle in an exhibition of a film at Ajanta Cinema, Swati Bhangalia and her

team tackled the sensitive case dutifully. Later it was found out that the concerned guy deliberately made a Facebook post based on a message he received in a WhatsApp group. It was also found out that the WhatsApp message came to him in a chain format. The investigation is going on the technological front as to who first sent the message.

Traffic congestion has been a menace in this part of the city due to the ongoing Metro construction work. "We have strategised considering the ground reality. In most cases, the metro rail stations are on the main road. Our team is working round the clock to ensure seamless traffic in this part of the city. Near Karunamoyee, we have guard railed a part of the road for smoother auto-rickshaw movement during the market hours. Overall, we are coordinating with the police stations and stakeholders to reduce traffic," said Swati Bhangalia.

Regular patrolling and vigilance have been an excellent addition to this area.

In a very recent case, under the jurisdiction of the Parnasree Police Station, Kolkata Police has successfully nabbed a cyber racket involving OTP sellers, fake Aadhar card generators, and pre-activated SIM card sellers and those in the digital wallet companies working on illegal terms to gain benefits. A resident of Parnasree complained that his SBI Yono phone number was changed without his authorisation and Rs20 lakh was withdrawn from his account in a few hours. He made a mistake by clicking on a vicious link sent by a fraudster to complete his bank KYC. Under the able leadership of IPS Swati Bhangalia, the officers of Kolkata Police busted the racket, which unearthed a new trend of cybercrime in India as a whole, involving a bigger scale of bank fraud.



Capacity Building: Answer to Threats and Vulnerabilities in Cyber Domain

Etymologically, capacity originates^[1] from the old French word *capacité* meaning ability to hold. Therefore, capacity building means, one's effort to build or scale up one's capability to hold. In the context of a nation's cyber-security posture, capacity building means to scale up the internal capability of

the nation at large to keep the cyber domain safe and secure.

In this essay on capacity building, an attempt will be made to discern as to what is understood by this oft-quoted cliché and how

Sanjay Kumar Das
WBCS (Executive),
State Information Security Officer,
Director, West Bengal Cyber Security
Incident Response Team,
Member-Secretary, Cyber Security Centre
of Excellence & Joint Secretary,
Information Technology Department, Govt
of West Bengal

to leverage the existing structure to ensure a robust ecosystem of safety and security of the cyber-domain.

A Bird's Eye View

In the Government Sector, capacity building is generally equated with training of human resources. Across the country, most of the State Governments have a dedicated setup for combating cyber-threats to their public ICT infrastructure. Presently, at the national level, Central agencies/ organisations viz. CERT-In[2] under MetiY; NCIIPC[3] under NTRO; CyCord[4] under MHA; Resource Centre for Cyber Forensic – India (RCCF-I)[5] under C-DAC Thiruvananthapuram and many other agencies undertake various types of trainings to develop the internal capability of stakeholders related to the cyber-security ecosystem. The Information Security Education and Awareness (ISEA) [6] is an awareness generating-cum- training programme under MetiY and implemented by C-DAC Hyderabad. Similarly, State Governments viz. Kerala through their State IT Mission; Maharashtra through their Maharashtra Cyber; Karnataka through their Cy-Sec; Telangana through their Cybersecurity Centre of Excellence; Andhra Pradesh through their Cyber Security Operations Centre; West Bengal through their Cyber Security Centre of Excellence among others undertake training programmes on Cybersecurity to upskill the stakeholders.

When one studies various efforts undertaken by Government agencies across the nation, it becomes clear that capacity-building imparts maximum thrust upon rolling out training programmes for enhancement of awareness among stakeholders rather than creating long-term assets in the form of upskilled human resources with cutting-edge technology skills. The nature of capacity building efforts undertaken by key Government agencies along with their target

No.	Organisation	Target audience	Type
1	ISEA, MetiY & C-DAC Hyderabad	Govt Employees Teachers & Students Citizens	Information Security Awareness
2	CyCord, MHA	Law Enforcement Agencies	Cyber Crime Awareness & Mitigation Techniques
3	RCCF-I, C-DAC Thiruvananthapuram	Law Enforcement Agencies, Armed Forces etc.	Forensic Tools and Techniques (Short term)

audiences have been enumerated below:

Various State Governments across India undertake similar training programmes. However, hardly any of them were able to instill cutting-edge skill within the participants. These training at best could increase either general or specific level of awareness in them regarding cybersecurity or cyber-forensic.

While in academic sector, institutions viz. Gujarat Forensic Sciences University (presently rechristened as National Forensic Sciences University)[7], various IITs (especially Kanpur IIT), NITs, IIITs including State as well as Central Universities are primarily involved in capacity building of students and professionals. Here, capacity building is equated with academic upgrade rather than up-skilling in a live environment. Therefore, academic excellence is often achieved but their impact on cybersecurity posture of the nation remains mostly neutral.

On the Industry front, the situation is different. Here, capacity building means preparing for what is required by the clients. In true sense, it is outcome oriented. Industry follows a hybrid approach, mixing acquired knowledge with employees' experience. This heady concoction usually brings results.

Public ICT Infrastructure is an ecosystem comprising Assets, Systems, Process and Manifested Applications. Capacity building is an effort to seamlessly scale up this entire gamut of ICT infrastructure. During the first decade, post the enactment of IT Act in 2000; the general administration across the nation became busy in procuring ICT assets more out of compliance than necessity because the applications i.e. eGovernance service delivery activities were only at their nascent stage. Yet, this procurement had a positive impact as foreign multinationals came to the country, set up shops, and support services increased exponentially. The IT boom was fuelled by establishment of private engineering colleges and outsourced service industry e.g. BPOs, KPOs, LPOs etc. Commercial organisations were created and common citizens were made privy to the benefits of application led service delivery. IRCTC[8] became a household name. During the second decade that ran up to the rolling twenties; attention was given extensively to process as well as applications. From device dependent software a paradigm shift was witnessed when software as a service (SaaS) started to invade everyday life. This trend leverages establishment of various online stores, code-repositories and application sharing platforms. Also,



Original Equipment Manufacturers (OEMs) put in astronomical sums of money into development of ready to use platforms for providing services to citizens ranging from hygienic food delivered at door step to transport aggregation service; from education to infotainment; virtually everything from birth to death. In the meantime, a large community working on free and open source applications (FOSS) [9] had parallelly came into existence that the OEMs now could not ignore. As another decade sets in with the 2020s, the OEMs have commenced integrating their platforms with open source applications[10]. This has brought the Government initiatives to a cross-road which had never been charted before. The Government organisations, faced with this technology avalanche, often have to rely on the external consultants as their internal manpower could hardly keep pace with the changing technological advancement. That creates a knowledge gap and by involving external experts, getting used to them, depending upon them now leads to a vicious cycle of blind dependence. Government organisations tend to invest more on engagement of consultants rather on capacity building of

internal resources. To support this stance, refuge is often taken behind the change-averse attitude of the government employees.

Based on the above, it can be easily inferred that capacity building in cyber security exudes different meanings for different sectors. To the Government, it is primarily soft skill development training; to academia, it is a qualification building exercise while in industry, it is sustained outcome based and demand driven skill enhancement. Though capacity building also refers to scaling up of ICT infrastructure, the nuance of associating it with training and skill-development pervades the former. Overall, it can be said that capacity building is the process by which individuals and organizations obtain, improve, retain the skills, knowledge, tools, equipment and other resources needed to do their jobs competently.

Demand of Today and Tomorrow

Ease of Use and Security are two sides of the same coin.

During the second half of the last decade, application development

for public service delivery witnessed an abnormal growth. Demonetisation[11] coupled with Digital Bharat Mission (Digital India)[12] largely fuelled it. Government establishments were now forced to usher in SaaS, PaaS and IaaS platforms and integrate with existing eGovernance applications to cater to the burgeoning demand felt across the country. Thus, hybrid and agile application development posture were adopted and petabytes of data are generated and stored in cloud-based applications and storage repositories. At present, more than 27.5 thousand Indian App (application) Developers are regularly publishing on Google Play Store and their collective applications hosted on it are more than 1.37 lakh[13]. Government of India now boasts many of their homegrown platforms under the aegis of National eGovernance Division (NeGD)[14] and National Informatics Centre (NIC)[15].

These applications are developed on versatile platforms. When they are led and developed by consultants or big corporations, they are mostly developed on proprietary platforms (.Net et al) or OEM led Rapid Application Development Platforms (RADPs

e.g. GSuite, OutSystem, Zoho et al). On the other hand, when they are developed by NIC or for that matter, State-level organisations with shoe-string budget, these public service delivery applications, which are mostly process flow based, are often developed on open source platforms e.g. LAMP[16] (Linux-Apache-MySQL-PHP).

With ever-increasing appetite for service delivery applications; proper development strategy takes a backseat with security by design being largely ignored and auditing for procuring safe to host certificates before the launch of any application becoming the only opportunity to check for security conformity and compliance. In order to launch an application within an ambitious timeline, often this safe to host auditing is neglected too by invoking overriding powers of the executive authorities. One-upmanship plays a crucial role in such situations with administrators, while remaining unconnected with the application development process and developers being forced to launch applications ignoring security conformity. Yet, this upscaling effort has brought in Development Operations standards but the need of the time is DevSecOps which is loosely defined as introducing security earlier in the life cycle of application development, thus minimizing vulnerabilities.[17]

This apparent avoidance of conforming to security pre-requisites often ushers in threats and vulnerabilities. The primary reason for such negligence stems from lack of knowledge on the part of internal resources and lackadaisical approach of consultants who prefer speed of delivery over security. Even when the CERT-In advises to undertake regular Web Application Security Audit (WASA)[18] most of the Government applications fail to



comply because

1. CERT-In empanelled Security Auditors are very few[19]
2. Regular audits put burden on the O&M expenses
3. Engagement is a cumbersome process
4. Developers remain perennially unwilling to put resources for security compliance
5. Lack of internal capacity compels outsourcing of security compliance too.

Over 5,000 government websites are currently active [20] and it has recently been brought to the notice of the Parliament that most of these websites lack regular security auditing and/or does not possess valid Secure Sockets Layer (SSL) certification. An SSL certificate encrypts the data that goes from a user's computer to the target website and back. Based on the same, MeitY on 26 August 2020 issued an advisory that states inter alia 'All the Government websites should have valid SSL certificates which are also recognised by the browsers.' This clearly means, Government web-applications ought to be regularly audited and ought to possess valid SSL

certificates. MeitY categorically directed NIC to ensure compliance of the above advisory. The question remains, what time NIC would take to ensure compliance of the said advisory. The answer is indefinite. This is possible only when all Government organisations ensure the following:

1. Ushering in DevSecOps standards in application development
2. Upskilling existing human resources and create a skill-pool in the organisation for ensuring benchmarked security posturing of the organisation and its applications
3. Conducting 'On the Job' (OJT) trainings to generate awareness and create the need
4. Engagement of CERT-In empanelled auditor for regular web-application-audit.

It is thus understood beyond reasonable doubts that exponential growth in application dependent service delivery has increased Ease of Use but failed to take care of security of applications in particular and ICT Infrastructure in general. This was fuelled by over-dependence on external subject-

matter experts and lack of capacity of internal resources.

Answer to Threats and Vulnerabilities in Cyber Domain

Capacity Building is an easy and effective answer to various threats and vulnerabilities that cripple web-applications and public ICT infrastructure in public domain. To corroborate this statement, a Use-Case Analysis is laid down below.

A. Use Case: Capacity Building efforts of Cyber Security Centre of Excellence (CS-CoE), West Bengal[21]

B. Description of Capacity Building Efforts: Capacity Building involves upskilling of internal resources besides enhancing sense of ownership among stakeholders. At CS-CoE, Awareness Generation & Capacity Building is the primary vertical among the Pre-cyber-incident initiatives. Coupled with Cyber Security Assurance vertical, various capacity building efforts are launched to achieve the target of Meeting in the Middle. The concept of Meeting in the Middle is to bring all stakeholders unto a common ground in-between. For ensuring cyber-safety of public ICT infrastructure, it is important

that stakeholders viz. citizens from various walks of life, law enforcement agencies and civil government employees are on one hand (a) made aware about cyber-security posture of the State in sync with the country; (b) enthuse to learn and implement from best practice use cases; (c) assess own ability to upskill for sustainable knowledge assimilation; (d) identify what skill-building training / academic courses would suit that need; (e) connect with concerned effort to undertake capacity building exercise; (f) undergo assessment and certification programme; (g) augment the efforts under Cyber Assurance Programme and thereby (h) ensure cyber-safety of the State as well as the country. On the other hand, the vertical Cyber Security Assurance ensures identification of threats and vulnerabilities in the ICT Infrastructure through the conduct of Web Application Security Assessment/Audit (WASA) and (ICT) Infrastructure Security Assessment / Audit (ISA). Some of the findings are enumerated underneath for better understanding.

350 counts of different type of vulnerabilities have been found to exist in 125 Web Portals /

Applications owned by 90 Departments, Directorates & other Govt organisations.

- Click jacking –65 counts
- Email spoofing: Missing SPF Record / Missing DMARC record / Misconfigured DMARC record –58 counts
- Security Misconfiguration – 45 counts [HTTP Strict Transport Security, Path Disclosure and Improper Error Handling, Server Version Disclosure, Technology Version Disclosure, OTP Bypass, Server status exposure]
- Sensitive Information Disclosure – 32 counts
- Directory Listing – 15 counts
- SQL Injection –12 counts
- Weak Cipher (Sweet32) – 10 counts
- Cross site scripting –8 counts etc...

Some network vulnerabilities found in these exercises are enumerated below:

- SSL Certificate – Untrusted
- SSL Self-Signed Certificate
- SSH Protocol Version 1 Session Key Retrieval
- SSL Version 2 and 3 Protocol Detection
- SSL Medium Strength Cipher Suites Supported (SWEET32)
- Terminal Services Encryption Level is not FIPS-140 Compliant
- Cisco Outdated IOS Affected with Multiple Vulnerabilities
- SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
- SSL RC4 Cipher Suites Supported
- SSLv3 Padding Oracle on Downgraded Legacy Encryption Vulnerability (POODLE) etc...



While some of the server-side vulnerabilities are:

- SSL Self-Signed Certificate
- SSL Medium Strength Cipher Suites Supported (SWEET32)
- SSL Certificate Cannot Be Trusted
- SSL RC4 Cipher Suites Supported
- Terminal Services Encryption Level is not FIPS-140 Compliant
- SSLv3 Padding Oracle on Downgraded Legacy Encryption Vulnerability (POODLE)
- SSL Version 2 and 3 Protocol Detection
- SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
- Microsoft RDP RCE (BlueKeep)
- PHP Version Outdated Affected with Multiple Vulnerabilities
- SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened encryption) etc...

Some of the vulnerabilities found in applications hosted on the State Data Centre:

195 counts of vulnerabilities found in 33 Virtual Machines (VMs).

- The remote service encrypts traffic using an older version of TLS – 18 counts



- The SSL certificate chain for this service ends in an unrecognized self-signed certificate – 17 counts
- The remote service supports the use of medium strength SSL ciphers – 16 counts
- The SSL certificate for this service cannot be trusted – 16 counts
- An SSL certificate in the certificate chain has been signed using a weak hash algorithm – 15 counts
- The community name of the remote SNMP server can be guessed – 15 counts etc.

Based upon these findings; two separate tracks of capacity building exercises were undertaken at the CS-CoE. Firstly, On the Job

Training[22] (OJT) – Under this effort, Government employees in all those Departments, Directorates, State and District level Govt organisations where the ISA and/or WASA exercise has been undertaken, are trained at their respective workplace. These physical interactions include classroom teaching as well as hands-on training. All employees are trained on Cybersecurity Hygiene on the first day. Only the application users among them are trained on Endpoint threats and vulnerability mitigation techniques on the second day while on the third day, System Administrators & Approvers are trained Basics on Application & Network Security and Vulnerability mitigation – primarily on how to read, assess and implement recommendations of Audit.

Secondly, owing to the Covid-19 pandemic led lockdown; an online course namely Cyber Swadhinata Programme[23] has been successfully rolled out for Government technical resources across the State that imparts training similar to OJT and beyond. In the said training and also in the OJT, vulnerabilities often found at endpoint devices used for office work during the Assessment cum Audit exercise, are discussed and





their mitigation techniques are taught.

Some of the desktop vulnerabilities found in these exercises are:

- User accounts have non-expiring passwords
- Windows Security Patches Not Updated
- User accounts have simple passwords
- Out-dated Windows 7 OS is Used
- Out-dated Windows XP OS is Used
- Shared Directory Access

C. Capacity Building Efforts in Law Enforcement Agencies:

Capacity building effort for law enforcement agencies require a special mention. Primarily because this disciplined workforce act as per Standard Operating Procedure (SOP) laid down for them and trained to work according to the same. Keeping this in view, efforts were undertaken to imbibe the Meeting in the Middle concept here too. First Responder Training (FRT)[24] is designed to upskill police personnel from the rank of constable up to Sub-Inspectors so that each and every cyber-crime complaint is properly attended to. FRT ensures that any citizen

desirous of lodging a cyber-crime related complaint is guided properly to identify and preserve the evidence and thereby lodge an actionable complaint. The training is a class-room one while at present the same is being readied to be imparted over digital platforms. On the other hand, Detailed Responder Training (DRT) is designed for the cybercrime investigators i.e. for the police personnel from the rank of Inspectors and above. Therein via class-room teaching alongside extensive laboratory activities involving used cases, outcome-based skill-imparting training is provided in batch-mode. At present, the same is also being readied to be imparted over digital platforms. Both these training curricula are approved by the Home and Hill Affairs Department and the Certification provided post assessment, conducted at the end of training, is entered in their respective Service Book. Similarly, Cyber Security Orientation Training (CSOT)[25] is imparted to all directly recruited Sub-Inspectors while they are in their 18-month orientation training. This is a modified version of FRT and therefore, these officers while on posting in police stations across the State ensure proper identification

and reporting of every cyber-crime.

While skill-building exercise is on for in-service personnel; capacity building exercise in true sense has also been adopted to increase the infrastructure of cyber-forensic activities. This way Meeting in the Middle is achieved. All 31 Cyber Police Stations across the State are provided with original tool(s) for CDR/IPDR analysis. Four police personnel from each of the Police Stations are trained on the said tool(s) after those tools are procured via price discovery and installed in respective machine at those Police Stations. Customised course curriculum is prepared and training is imparted with continuous assessment. Post- assessment, certification as to their ability to use those tools to analyse cyber-crime evidence is awarded too. On one hand, FRT and DRT make these personnel conversant on cyber-crime reporting and investigation while on the other, tool-based analysis of evidence collected and collated lead to evidence archiving and submission during trial which eventually increases chances of conviction.

Setting up a second Cyber Forensic Lab was a great leap toward achieving self-sufficiency in

capacity building. The new, state-of-the-art, State Cyber Forensic Laboratory was inaugurated on 8th September 2020 with advanced machines and tools. A month-long orientation training of Police personnel drawn from Criminal Investigation Department [26] (CID), was conducted on a customised course developed and imparted by CS-CoE, in line with Gujarat Forensic Sciences University. The said lab has commenced receiving evidence, analysing them and initiated a process for laboratory certification from MeitY, Govt of India. Third-party involvement is absent as the cyber forensic lab is run and managed solely by the CID, West Bengal with infrastructure, technical and up-skilling support from the CS-CoE.

Capacity building cannot be complete without future ready human resources, which has been discussed in detail beforehand. CS-CoE has in the meantime collaborated with C-DAC Kolkata and **Maulana Abul Kalam Azad University of Technology (MAKAUT)** [27], West Bengal to roll out various curricula for the academia as well as professionals. Maulana Abul Kalam Azad University of Technology has vested CS-CoE with the vetting responsibility for all their courses on cyber-security. In the midst of that, it was felt that threats and vulnerability management activities require a huge number of technical manpower who are hands-on. The Cyber Crime Magazine [28] quotes NASSCOM [29], the consistent growth in cybercrimes and rapidly increasing demand in the Indian cybersecurity segment will require 1 million cybersecurity professionals by 2020. Yet it fails to identify that most pass-outs from Technical Colleges and Universities across the country with Cyber Security specialisation, tend to get



absorbed in big corporates while mid-sized companies remain ever hungry of qualified cybersecurity professionals to uplift their security posture. To address this burgeoning demand and build capacity for this left-out sector comprising MSMEs and Start-up companies; CS-CoE created tailor-made Diploma Course on Information Security and Cyber Forensics for the West Bengal State Council on Technical and Vocational Education and Skill Development [30] (WBSCTVESD) which received AICTE approval and being rolled out in Polytechnic Colleges across the State from 2020-2021 academic session.

Nowadays, physical threat to physical assets has been replaced by digital threats to both physical as well as digital assets using the cyber domain and that's why safety and security in the cyber-domain is of utmost necessity. Based on this perception, CS-CoE has created a Vocational Level Certification Course for the Security Guards guarding physical assets viz. Banks, ATMs, Office buildings etc. in order to make them aware of digital threats, thwart attempts on physical and digital assets, help organisations follow best practices on Cyber Hygiene, Operating Centralised Building Management Systems among various other

activities. This way frauds and theft in the digital domain would come down drastically. WBSCTVESD has approved [31] the course Cyber Guard and the same is being rolled out through various Vocational Training Centres across the State. Through this, the State Government envisages to up-skill existing Security Guards and increase their employability.

EPILOGUE:

Capacity Building has versatile connotations. Confining it to mere training or skilling would be grossly unjust. Funding requirement for tiding over the necessity of technology upgrade that leads to infrastructure obsolescence has become a prime concern for Governments. As commercial entities are facing cyberattacks very often, procurement of security tools and technologies feature at the top of their agenda. But Governments are caught between choosing security over basic necessities of the citizens. Thus, the dire requirement for upskilling of internal resources is felt hard, who would help Governments adopt a middle path and ensure security with lesser dependence on tools and technologies. The above strategy successfully proves this point.

Recommendations for incorporation of the above use-case based strategy in the proposed National Cyber Security Strategy of 2020 was shared with the National Cyber Security Co-ordinator (NCSC)[32]. Up-skilling of human resources[33] available with the CS-CoE by allowing them to pursue skill-development curricula from BSI, ISAC-NCIIPC, ISEA-MeitY, ESCI-Hyderabad, DSCI, DIAT-Pune et al prove with certainty the strategy proposed here.

TAKEAWAY:

Capacity Building in cyber security domain needs to be seen as an effort to enhance inherent capacity of every organisation both infrastructure as well as human resource wise, so that public ICT assets including applications and data are kept safe and secured in the face of relentless onslaught of cyber intrusions from outside as well as from within. Funding is necessary for upscaling of infrastructure, when the strategy enumerated

above is followed to the 'T', the dream of attaining Cyber Safe Bengal – Cyber Safe India will soon turn into a reality.

ACKNOWLEDGEMENT:

Greatly indebted to our Dept of IT&E, the CS-CoE, West Bengal Police, Kolkata Police, CID West Bengal, Webel, SNLTR, and all our colleagues & professionals working with us, round the year. •

- [1]<https://www.etymonline.com/search?q=capacity>
- [2]<https://www.cert-in.org.in>
- [3]<https://www.nciipc.gov.in>
- [4]<https://www.cycord.gov.in>
- [5]<http://www.cyberforensics.in/default.aspx>
- [6]<https://www.infosecawareness.in/>
- [7]<https://www.gfsu.edu.in/>
- [8]<https://pib.gov.in/Pressreleaseshare.aspx?PRID=1579186#:~:text=Online%20ticketing%20through%20Indian%20Railway,address%20given%20by%20the%20passenger.>
- [9]<https://fsci.org.in/>
- [10]<https://opensource.microsoft.com/>
- [11]<https://www.indiabudget.gov.in/budget2017-2018/es2016-17/echap03.pdf>
- [12]<https://www.digitalindia.gov.in/>
- [13]<https://42matters.com/india-app-market-statistics>
- [14]<https://negd.gov.in/>
- [15]<https://www.nic.in/projects-all/>
- [16]<http://www.lamp-platform.org/>
- [17]<https://www.csoonline.com/article/3245748/what-is-devsecops-developing-more-secure-applications.html>
- [18]https://www.cert-in.org.in/PDF/guideline_auditee.pdf
- [19]<https://www.cert-in.org.in/s2cMainServlet?pageid=CERTEMPANEL>

- [20]<http://goidirectory.nic.in/index.php>
- [21]<https://cscoweb.gov.in>
- [22]<https://cscoweb.gov.in/activities/ojt>
- [23]<https://events.nltr.org/>
- [24]<https://cscoweb.gov.in/activities/frt>
- [25]<https://cscoweb.gov.in/activities/csot>
- [26]<https://cidwestbengal.gov.in/>
- [27]<https://makautwb.ac.in/>
- [28]<https://cybersecurityventures.com/india-will-need-to-fill-one-million-cybersecurity-jobs-by-2020/#:~:text=The%20National%20Association%20of%20Software,million%20cybersecurity%20professionals%20by%202020.>
- [29]<https://nasscom.in>
- [30]<http://www.wbscvet.nic.in/>
- [31]Certificate of appreciation received from WBSCVET for creation of these professional and vocational courses.
- [32]Certificate of appreciation received from the NCSC for sharing the above recommendations.
- [33]Capacity building achieved so far: 1800+ Police Personnel Trained, 9500+ Government Officials trained, 7200+ teachers/professors/faculty members trained, 25000+ Students Participated in various events, 250+ CII managers trained, 300+ Bank managers trained and 9500 participants attended in various events under Citizen's Awareness & Skill Development

Cyber Security Centre of Excellence (CS-CoE)

(<https://cscoe.itewb.gov.in>)



Initiatives of CS-CoE & CSIRT

Law Enforcement Agencies

(1,800 + Police Personnel Trained including 500 + from Kolkata Police)

- First Responder Training (FRT) for SIs, ASIs and Constable of Police.

- Detailed Responder Training (DRT) for Inspectors, DySPs and ACPs of Police.
- Cyber Security Orientation Training (CSOT) for Direct Recruit SIs of Police.
- Training on Secured Coding

Practice Framework for Developers and Coders of

- Training of police personnel on CDR/IPDR forensic tools for Cyber Police Station Personnel.
- Cyber Forensic preparatory training for CID Officials of WB Police, engaged presently with the Cyber Forensic Lab at SDF Building,



Government Officials

(9,500 + Government Officials Trained)

- On the Job Training (OJT)
- Cyber Swadhinata Programme – Training on Cyber Incident & Detection
- Basic Training on Cyber Security and Cyber Hygiene practices



Teachers

(7,200+teachers/professors/faculty membersTrained)

- Cyber Shikshak - a Cyber Security Awareness Training programme for the teachers of West Bengal

Students

(25,000 + Students Participated)

- ✓ Cyber Sahajpath - a Cyber Security Awareness Training programme for the students
- ✓ Hackathon
- ✓ Secure Bengal (Month long learning opportunity and Mega hackathon)
- ✓ Cyber Hygiene Training Programme for Emerging Youth

CII managers

(250 + Officials Trained)

- ✓ Training for State's CII managers

Bank managers

(300 + Officials Trained)

- ✓ Training for Bank managers

Citizen's Awareness &

Skill Development

(9,500 participants attended in various events)

- International Kolkata Book Fair
- Milan Utsav
- Kreta Suraksha Mela



- Swyamsiddha Mela
- Jungle Mahal Utsav
- Cyber Hygiene Drive at Durga Puja Pandals
- Crossword Puzzle Challenge
- Cyber Awareness Slogan Contest
- Cyber Awareness Poster Contest
- ✓ Pledge on Data Privacy (105,000+people have undertaken)
- ✓ Cyber Security Pledge (50,000 + people have undertaken)
- ✓ Observed Data privacy Day
- ✓ Observed National Cyber Security Awareness Month (NCSAM) October
- ✓ Awareness campaign for Senior Citizens
- ✓ Organised many interactive live-in programmes at Akashbani and Friends FM radio channels reaching more than five crore listeners across the State and the World via live-streaming over social-media



Publications

- ✓ Cyber Hygiene Handbook in Bengali, English and Hindi
- ✓ Cyber Sammohan Comic Book in Bengali, English and Hindi
- ✓ Cyber Security - A knowledge for safer tomorrow - in Bengali and English
- ✓ E-Book of Cyber Security Incident Response and Mitigation Advisories

West Bengal Cyber Security Incident Response Team (WB-CSIRT)

(<https://csirt.itewb.gov.in>)

- **Information Security Officer (ISO), Information Security Technical Officer (ISTO) and Incident Response Team (IRT)** for each department/district of the State Government were collected and maintained.
- **West Bengal Cyber Yoddha Team**, a digital task force under West Bengal Cyber Security Incident Response Team (WB-CSIRT) was formed.
- Identification of **Critical Information Infrastructure (CII)** for the State is in progress.
- State's **Cyber Crisis Management Plan (CCMP)** was placed and approved.
- Six incidents took place and were addressed as per the guidelines of the **Cert-In**
- On receipt of the POC from **NCIIPC, Cert-In, etc.** Remediated 300 + identified vulnerabilities.



Awards received by Cyber Security Centre of Excellence (CS-CoE) For CAPACITY BUILDING and CYBER ASSURANCE PROGRAMME



DSCI Excellence Awards 2021

Cyber Security Centre of Excellence, Department of Information Technology & Electronics, Government of West Bengal received the DSCI Excellence Award under the category Cyber Security Awareness - Government/NGOs in the year 2021.

DSCI Excellence Awards 2020

Cyber Security Centre of Excellence, Department of Information Technology & Electronics, Government of West Bengal received the DSCI Excellence

Award for Raising Security Awareness.

Cyber Security Centre of Excellence, Department of Information Technology & Electronics, Government of West Bengal is also a finalist of the DSCI Excellence Award for Best Security Practices in Government Sector.

International Outstanding Security Performance Awards (Cyber OSPAs) 2021

Cyber Security Centre of Excellence, Department of Information Technology & Electronics, Government of West

Bengal is also a finalist of the first-ever Cyber OSPAs for various categories like Outstanding Cyber Security Team, Outstanding Cyber Security Training/Awareness Initiative, Outstanding Police/Law Enforcement Initiative, etc.

2nd Elets India Transformation Summit & Awards 2021

Cyber Security Centre of Excellence, Department of Information Technology & Electronics, Government of West Bengal received 2nd Elets India Transformation Summit & Award for the project CYBER SAFE BENGAL, CYBER SAFE INDIA

under the category Cyber Security Initiative.

Indian Express Digital Technology Sabha Award 2021

Cyber Security Centre of Excellence, Department of Information Technology & Electronics, Government of West Bengal received the Indian Express Digital Technology Sabha Award 2021 under Enterprise Security category.

Governance Now 4th Digital Transformation Awards 2021

Cyber Security Centre of Excellence, Department of Information Technology & Electronics, Government of West Bengal received Governance Now 4th Digital Transformation Awards 2021 for the project Cyber Assurance Programme under the category Cyber Security Initiatives.

SKOCH Award 2021

Cyber Security Centre of Excellence, Department of Information



Technology & Electronics, Government of West Bengal received SKOCH Order-of-Merit for the project Cyber Assurance Programme.

Elite Excellence Awards 2020

Shri Sanjay Kumar Das, WBCS(Exe.), Joint Secretary, IT&E Department, Govt. of West Bengal and Member-Secretary, CS-CoE received the Elite Excellence Awards 2020.

National Cyber Security Scholar Programme 2020

Five officials from the Cyber Security Centre of Excellence, Department of Information Technology & Electronics, Government of West Bengal attended the ISAC and MDI National Security Fellowship Programme organised by the Information Sharing and Analysis Centre (ISAC). Shri Sanjay Kumar Das, WBCS(Exe.), Joint Secretary, IT&E Department, Govt. of West Bengal and Member-Secretary, CS-CoE topped the programme and received the MDI-ISAC Scholar High Honours for his performance in the entire programme. Shri Sanjay Kumar Das and team also received the award for innovative paper which was written on Capacity Building.

Elets Education Innovation Award 2022

Shri Sanjay Kumar Das, WBCS(Exe.), Joint Secretary, IT&E Department, Govt. of West Bengal and Member-Secretary, CS-CoE received the Elets Education Innovation Award 2022 instituted jointly by Haryana State Govt at Panchkula, Chandigarh, Haryana on 26th May 2022.



Vigilant Bengal Officer Alerts Police About Cyber Fraud; Accused Arrested

Cyber frauds had tried to trap a senior government official of West Bengal by sending him messages on his mobile that he had won a big amount in the WhatsApp Global 2020 contest.

The message was sent on 21/06/2020 at around 15:33 hrs when the accused persons entered into criminal conspiracy by sending a fake message on his mobile number 708514****, informing him that his WhatsApp number has won Rs 2.75 crore in the WhatsApp Global 2020 contest, asking him to send his details to the Email address rbidelhi@rbigovt.in.

But the receiver of the said message became alert and did not fall prey to such allurements. In doing so, the accused person used forged and fabricated documents using electronic records/documents and computer resources to pretend to be genuine.

The public domain registry was approached to get the details of the questioned domain rbigovt.in. A reply was received wherein it was revealed that the alleged

email address rbidelhi@rbigovt.in is associated with mobile number +91 98719**** and it could be learnt from Airtel that the number was issued in the name of one M. Kumar of New Delhi.

Also one IndusInd Bank Account vide Account no 10002437**** could be traced along with one Fino Bank Account.

In the course of investigation, it could also be learnt that few transactions from both the IndusInd Bank Account and that of the Fino Bank were being done

with one ICICI bank Account vide No: 001105**** which is associated with one phone number 989992**** active in Delhi Circle.

A raid was conducted at Tigri PS, New Delhi area along with a team of Cyber PS. During raid, the said M Kumar was interrogated who confessed that he was running a mobile recharge shop in Raju Park area, New Delhi and identified the alleged number 989992**** to be of one John **** alias Simon (34 Yrs) of Krishna Park, PS—Tigri, New Delhi.

After proper search, the mobile phone was found from the possession of John and seized. After proper interrogation, John ***alias Simon was arrested for having complicity in this case. The accused could not produce any original or photocopy of his passport or Visa. From his possession, one laptop was found.

The accused person was closely interrogated and it could be ascertained that he not only sent the false messages to the mobile number of the complainant of the instant case, but also repeated the said offence and cheated many innocent persons for money.

It could also be ascertained from the statement of the accused person that he had fraudulently procured the Visa in his name and subsequently stayed in India without any valid Visa. Steps were taken to verify whether any genuine passport and visa were issued against his name or not. During investigation, the Director, Western Africa Division, Ministry of External Affairs and Deputy Commissioner of Police, Foreigner Regional Registration Officers were approached to ascertain whether any genuine passport and visa were issued for him or not.

The reply from the Director, Western Africa Division, Ministry of External Affairs was received wherein they could not confirm any visa or passport number.

Meanwhile, the accused was thoroughly interrogated in police custody in the light of the instant case. On interrogation, he spilled the beans. The accused person accessed the BigRock to register the domain rbigovt.in using the Big Rock ID: olilviaparker87@gmail.com to commit the offence.

He took charge of some incriminating screenshots as the exhibits of this case and kept a case diary.



The team of Cyber PS again approached the Delhi Police to conduct a search/seizure but neither device nor any copy of passport or visa could be recovered. As a result, Sec. 14 of the Foreigners Act 1946 was added with the existing sections of law in the interest of the case.

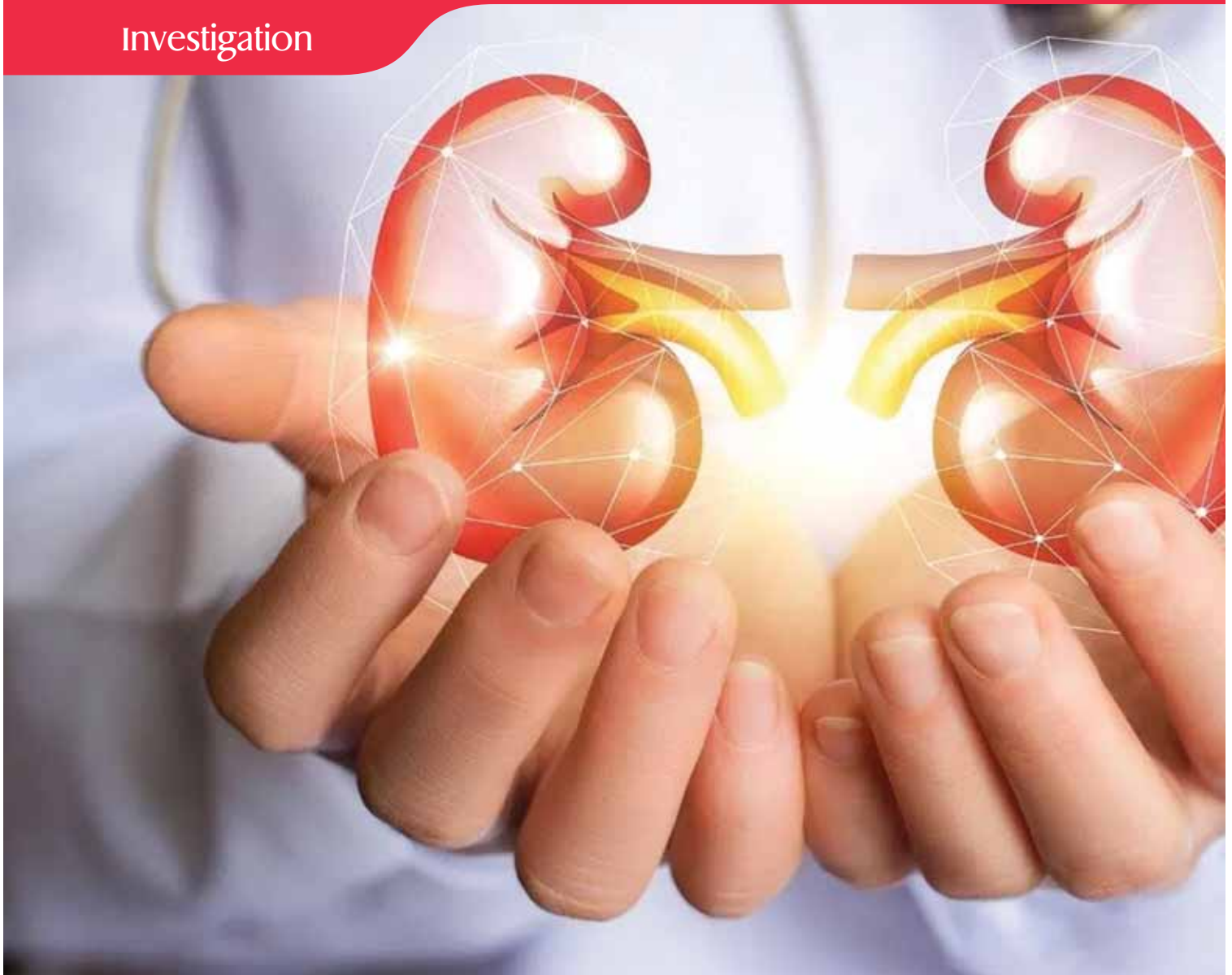
The electronic devices i.e laptop and mobile phone used by the accused person to commit the crime were analysed by different cyber forensic tools including Internet Evidence Finder (IEF), Image of the HDD was made using the FTK imager Lite and examined the same using Encase. Using Cellebrite his mobile phone data was extracted and it was found that he chatted not only with the complainant but also with several other men and cheated them on various pretexts. On being allured and duped by their false representation, Indians used to transfer a huge amount of money in the desired accounts of different banks to get the valuable gifts.

The accused person and his associates sent thousands of false lottery winning messages to unknown persons to lure them. If someone fell into the trap of their false promises, they extorted money from them on various pretexts. They had also sent the same kind

of tempting messages to the mobile no. of the Hon'ble Chief Justice of High Court, Calcutta.

The investigating agency submitted a charge- sheet within a very short span of time and the trial was completed. The accused person has been awarded a 6-month sentence and a fine of Rs. 40,000 was imposed by the Ld. Court of Chief Metropolitan Magistrate, Kolkata.

The investigation and detection of the said case was a tough task as the accused person used several mobile numbers to conceal his identity. Lots of beneficiary bank accounts were opened using forged and fabricated documents. Initially the police team did not get any clue. Later, on the basis of addresses given in the KYC documents, tower locations and IMEI trace, the IO and his team were able to identify the area from where the accused person was operating. Based upon the information from a mobile recharge point agent and calculating the exact tower location of the new number obtained from the mobile recharge agent, the location of the Nigerian accused could be fixed. The police team did hard work in Delhi and they camped at Delhi for around 10-12 days before succeeding in apprehending the accused person from his hideout.



Online Fake Kidney Racket Unearthed Nigerian National Held

The investigating wing of Kolkata Police cracked a fake kidney racket being run from outside the city and arrested a Nigerian national involved in the case.

According to the case, an accused person unauthorisedly created a fake website in the name of Fortis Hospital & Kidney Institute vide URL http://*****/home/discussion/ownieu/a_kidney_for_sale_making_profits_of_human_bodies/ using the logo of the hospital to appear genuine without

their consent and knowledge. A false and misleading advertisement was published on the hospital's website claiming as the representative of the hospital advising the general public for kidney donation stating that the hospital will pay for such donation with an intent to damage the reputation of the hospital.

Thereby the accused person committed offence U/S 66C/84B Information Act 2000 r/w Sec 419/465/468/469/471 IPC.

Investigation: During the course

of investigation, registrar of Godaddy.com was approached with a notice u/s-91 Cr.P.C and requested to provide complete particulars of the registrant of the questioned domain "disqus.com" vide URL: https://*****/home/discussion/ownieu/a_kidney_for_sale_making_profits_of_human_bodies/ including mode of payment done by the registrant at the time of domain name registration and also the IP address with date and time stamp with the email address of the questioned

with questioned mobile no. 95851**** was used on Disqus.com having url https://****/home/discussion/the-standard-digital-news/kidney-sale-cartels-harvest-more-body-parts-than-agreed and also found a hyperlinked page having url https://****/by/disqus-Tri6ROL5mZ/. During the search, some advertisements using the logo of Fortis hospital could be found as quoted "Genuine organ donors needed urgently, for an attractive price of 1.70 crore, Contact Dr Ian Hoffman of Fortis Hospital on at: MOBILE:+919585**** EMAIL:fortisre****@gmail.com".

Accordingly Google Inc. was approached to get the creation and login details (IP address with date and time stamps) of E-Mail ID fortisr****@gmail.com. Meanwhile, a reply was received from Godaddy.Com wherein they stated that to obtain the information sought in the letter, they required a request through CERT-In with an appropriate order from a court of competent jurisdiction.

Accordingly a prayer was made to the court of Ld. C.M.M, Calcutta for issuance of notice u/s 91 Cr.P.C as per the provision of Sec. 69 of Information Technology Act 2000 upon the Group Coordinator (Cert In), Cyber Law Division, Department of Electronics & Information Technology, as well as GoDaddy.com to provide the information in respect of questioned domain "disqus.com" vide URL : https://d****/home/discussion/ownieu/a_kidney_for_sale_making_profits_of_human_bodies.

The Ld. Court issued a notice to the concerned authority advising the Computer Emergency Response Team (Cert-In) to take necessary steps from their end to get required information. After receiving the reply from Cert-In and scrutiny, it could be learned that IP 116.202.23.62 was used to upload that questionable post.

In the course of investigation, a reply was received from Google Inc. wherein it was revealed that the questioned email Id fortisre****@

website in case the domain name was purchased online.

During investigation, a reply was from ATTN Domain Enquiries wherein they suggested to contact Mail.com's Legal Department through email ID LegalNotice@gmail.com.

Accordingly mail.com was contacted through mail ID LegalNotice@gmail.com and received a reply from Legallegal@1 and 1.com wherein they informed that they required US Subpoena to release the information in respect of domain consultant.com.

While search engines and social media sites, it was found that one advertisement





gmail.com was created using the IP 116.202.***.*** on 04/06/17 at 19:14:04—UTC in the name of Fortis Hospital Kolkata and registered with one mobile number.

During investigation several mobile numbers and 11 IMEI numbers were found. After collecting CDR's of all the mobile numbers and scrutinizing all the IMEI and CDR's it was found that all the numbers were located at a particular place called Nagenhally, Narayanpura of Bangalore.

After prolonged investigation, one Nigerian national was arrested from Nagenhally, Bangalore. From his possession two mobile phones fitted with four SIM cards including the mobile phones which were used in this case, one laptop, three pen drives and several incriminating documents were recovered.

During the probe, it was found that the accused person had published several fake advertisements using the logo of Fortis Hospital & Kidney Institute, Rash Bihari Avenue, Kolkata for donation of kidney and cheated innocent people and extorted money in the name registration fees, various organ transplantation cards/certificates etc. He impersonated himself as a member of the National Kidney Foundation.

Later, chargesheet was submitted before the Ld. Court after completion of investigation and trial was completed within a very short time. After trial, the Ld. Court sentenced the accused person to 2.5 years of jail, rigorous imprisonment and imposed a fine of Rs4.5 lakh.

The investigating agency primarily did not get any clue as the concern

domain service providers denied to give required data. The accused person used several mobile phones and numbers to conceal his identity. During the imaging process, it was not possible to unscrew the laptop to remove the HDD. Thereafter "**Paladin**" was used to create disk images in the read only mode of the laptop.

The investigation and detection of the said case was truly a tough task as the accused person used several mobile numbers to conceal his identity and the concerned web server provider refused to give the reply. Initially, the domain service provider refused to reply but later the IO was able to get the answer from Godaddy.com with the help of CERT-IN. The IO and his team took the help of different forensic hardware and software tools like **IEF, Paladin, Cellebrite, FTK Imager Lite** etc. for imaging and analysing the storage device of seized laptop, mobile etc. On forensic analysis, it was found that the relevant portion of the text was present in the laptop of the accused person. **Internet Evidence Finder (IEF)** was also used to trace the impression of creation of online advertisement. CDR/IPDR analysis tools i.e **C-5 CDR Analyser** help was extensively taken into this case. The investigating agency could crack the case and arrested the person within a short period of the said incident.





!!! Puja Greetings !!!

**PROTECT &
DISINFECT**

YOUR HOME & SURROUNDINGS



**DOCTOR'S
PHENYLE**

SALUTES **"THE KOLKATA PROTECTORS"**
FOR BEING WITH US **ALWAYS**

Cybercrimes and the Need to Maintain Digital Hygiene

Sunirmal Roy, Officer-In-Charge of Cyber Cell, Lalbazar Headquarters, Kolkata Police, discusses with our reporter Ranabir Bhattacharyya various aspects of cybercrime in the city and steps to maintain digital hygiene.

Cybercrime is no doubt an evolving segment of crime. The Cyber Cell of the Kolkata Police Lalbazar Headquarters is constantly looking at the new trends and possibilities, and

exploring options and procedures to decode them.

The biggest hurdle has been the awareness quotient. Many such cases of cybercrime can be avoided if people are simply aware of

the loopholes. From a policing perspective, it is also a learning process for us every day. The role of the police is indeed tricky as in most cases the servers are placed abroad, and the multinational companies take time to reply.



There is a common misconception that all cases of cybercrime are instances of random hacking. As far as the recent trends of OTP frauds are concerned, users are doped into sharing their data for fake KYC updates, including OTP and money from the victim's account is transferred to the fraudsters, without any prior knowledge of the victim.

All these cases call for digital hygiene which we highlight is of massive importance. We advise more and more cyber sensitisation campaigns involving senior citizens. We are always supporting with our knowledge and expertise and in the coming days, with a more guarded approach and ever vigilant Kolkata Police force, the cybercriminals will have a real tough time. We already have strict

laws and sections in IPC which have been effective.

In the coming days, we are indeed confident that cases of cybercrime will come down considerably. We have a list of recommended prevention measures for netizens. Along with that, we are constantly making people aware of hacking, computerised fraud and other computer-related crimes. Child safety is another key area we are always careful about even in the digital context. Using social media intelligently is a significant area for all of us in today's world.

Lastly, we keep on informing people on how to keep themselves safe online. The recent cases of fake call centres rightly point out the need to be aware of wrongdoings in the cyber world. •

In very few cases, we get positive replies. Data security, end to end encryption mode often hamper detailed investigation as companies don't share data which can be decisive in matters of digital fraud, and social media blackmailing.

Digital Illiteracy and the Prowling Cyber Criminals

The Officer-In-Charge of Parnasree Police Station, Soumo Thakur, talks to Ranabir Bhattacharyya of Team Protector, about a bank fraud case which unearths the modus operandi of cybercriminals

Cybercrimes have been a matter of great concern for the police in particular around the country, especially during the Covid phase. There are different types of cyber fraud cases. But the most trending and complicated among them is bank fraud. Many people have an opinion that their electronic devices are hacked in cases of bank frauds. In reality, this isn't the case. The culprits call the victims for fake KYC (Know Your Information), collect the OTP (One Time Password) and subsequently befool the victim and transfer money to their accounts.

The whole modus operandi

involves phone calls, and no remote computer or app has any role in it. In other words, digital illiteracy is exploited along with lack of consciousness remains the focal point in most such cases.

Earlier we had seen many such cases of cyber frauds using social media platforms like Facebook, WhatsApp or Instagram. In some cases, the victims are blackmailed as well. But in the case of bank fraud, illegal transactions happen in no time, making citizens vulnerable to such acts.

Throughout the year, we have been leading campaigns against all sorts of cyber frauds. From beat

meetings, online video conferences, and leaflets distribution to awareness campaigns in localities, we have used all modes of local communication to make people aware of the dos and don'ts in case of digital transactions.

Still, there has been a part of the local population, who has been befooled by cybercriminals. We decided to go into depth, opting for an offensive approach against the criminals who are operating digitally.

Recently, a middle-aged man, who is a senior manager in a financial institution, became a victim of such an unfortunate trap. He received a call from an unknown number, requesting urgent submission of KYC to keep his bank account



active. He shared the OTP he received and then his phone number was replaced by a different number for his savings account.

In no time, Rs 20 lakh vanished and transferred to another account, regarding which he had no clue. He approached the bank authorities, but the bank authorities failed to acknowledge the fact that there were several other accounts which were linked to his phone number.

A moment of miscalculation and misunderstanding paved the path for such bank fraud. Thereafter, we started an investigation and what we came across was a complete eye-opener for all of us.

Mode of Operation and Different Verticals

At Halisahar, we arrested one Partha Saha from whom we recovered 700-800 pre-activated SIM cards. No doubt, a SIM card is a key to any

cyber
fraud.

After interrogating Partha Saha and his associates, we came to know of the whole plot consisting of the pre-activated procurement individuals, mule accounts and their creation, phone calling and fraud and data collection. A minimum of 50-60 persons work in an organised way in any particular bank fraud.

The Telecom companies set targets for local distributors for selling SIM cards. To meet the target and get additional discounts, the company sales manager and distributors work together to get fake connections which get deactivated after a few months. In the initial level of verification, fake Aadhar cards and duplicate photographs are used. The call centre employees of the Telecom companies often are very casual and fail to identify the discrepancy. In reality, there is no particular algorithm to differentiate photos. The pre-

activated SIM cards are sold to cyber criminals once the target is fulfilled. At the very next level, the criminals buy OTP. There are several OTP buyer and seller groups on Telegram, each having more than 12,000 members. These OTP transactions are used mostly by the officers of the wallet companies to meet targets. Once they achieve their target, the OTPs are sold to cyber criminals. Once the victim's account is compromised, the money is transferred to mule accounts. Mule accounts mostly belong to poor people who don't use their accounts often and getting quick money, agree to lend their accounts for such illegal monetary transactions. From these mule accounts, money is withdrawn by ATM, and sent to the criminals via courier. Thus the whole racket works in a systematically organised format, where across all levels, culprits play an integral role. Distributors, area sales managers, officers of the wallet companies, and mule account holders - all are indirectly responsible for organised crime like bank fraud.



Crime Scenario in the Covid Aftermath

In a candid interview with our Reporter Ranabir Bhattacharyya, Officer-In-Charge Shiv Shankar Roy of Netaji Nagar Police Station, discusses policing in the post-COVID scenario and the neo-approach to community policing. Excerpts of the interview

In the COVID phase, many people lost their jobs. The situation is worse, not only in the organised sector but also in the unorganised sector.

The high rate of unemployment has played its part in the crime pattern. The tendency of committing a

crime has gone up alarmingly. Interestingly, as per the data, rather than traditional crime, we are witnessing more cases of online frauds, especially bank frauds. To tackle this menace, the entire police force is now getting training to handle them, what sections are to

be imposed on such complaints and the SOP has been shared as to how to put the best step in the interest of the citizens. We are now much better equipped with our 360-degree approach to handling complaints involving cybercrime. We have seen that senior citizens who leave alone



are most susceptible to such cases. The Netaji Nagar Thana is now focussing on direct connection with the senior citizens with round-the-clock support. We are seriously concerned and dedicated to sensitising them about the do's and don'ts. We have received several complaints of ATM frauds, OTP frauds and different types of digital frauds.

Last December, our Netaji Nagar Police Station Team caught a gang of bike thieves, which indeed was a great effort considering the kind of investigation the whole case demanded.

Last year, we were regularly receiving complaints of bike thefts. As our team was investigating every minute detail, we zeroed in on a local guy Abhradip Naskar. We kept a constant watch on his whereabouts. As we arrested him and interrogated him further, we came to know of his friend Rahul Mondal, based in Narendrapur. We nabbed Rahul from Canning. Both of them confessed to their active involvement in the crime. Their mode of operation was mostly night-centric. In Kolkata, due to space constraints, many people keep their two-wheelers on the road. These two culprits first used to take a recce of a particular area, marked the probable houses and then coordinated the whole theft.

In most cases, the bikes were taken to South 24 Parganas and in some cases, across the border to Bangladesh. Once we got their police custody, the team worked hard to recover the two-wheelers which were stolen from the Netaji Nagar area. Not only that, we also ended up recovering other bikes stolen by the gang. As of now, we have some recovered unclaimed two-wheelers.

Added to this, we also recovered two bikes stolen from Narendrapur area, which were later handed over to the Narendrapur Thana Police officials. It was indeed a moment of pride as the erstwhile DC SSD IPS Rashid Munir Khan congratulated us for our efforts.

The good thing is that now we have not come across any such cases of bike theft in the Netaji Nagar area. I am indeed thankful to my team at the Netaji Nagar Police Station for their consistent and dedicated effort in keeping the area safe and peaceful.

CLUB MUSLIN
AN EXCLUSIVE SHOW ROOM OF MUSLIN PRODUCTS

Exploring endless Fashion & Design of Muslin. Contemporary Brand of Eco-Friendly and earthy range of hand woven Muslin- the pride of Bengal - Visit & Experience

GRAMIN

West Bengal Khadi & Village Industries Board
12, B.B.D. Bag, Kolkata-700 001.
Website: www.wbkhvib.org.in



Taking Big Strides with Eco-Friendly Initiatives

Ranabir Bhattacharyya

The Kolkata Police has always been inclusively efficient about policing. Policing in the added area under the Kolkata Police has come under much focus since the inception of the new police stations.

The Sarsuna Police Station is one such police station which was inaugurated in 2014 and has come a long way, with a unique approach to policing. The Officer-In-Charge of Sarsuna Police Station, Siddhartha Chatterjee, candidly said, “This police station has been a fantastic addition to the Kolkata Police jurisdiction. The local aspirations have been served dutifully by the police personnel. Even though there are some similarities with the panchayat area, policing has been top-notch, serving the citizens with care and compassion, ensuring

safety and peace all across.”

In an interdepartmental competition organised by the Lalbazar Headquarters across various categories among all the police stations under the Kolkata Police. The main focus of the competition was to reassess the infrastructural facilities of the police stations based on various parameters which are integral to core policing and the scope and avenues to improve further.

The senior officers were the judges of the competition. There were four categories namely front office and green initiatives, malkhana, barracks and mess, back-office and Investigation Officer’s (IO) room. The Sarsuna Police Station came third in the malkhana section and second in the remaining categories.

Siddhartha Chatterjee further

added, “When I was transferred to the Sarsuna Police Station, I was delighted to see so much scope to explore and undertake green initiatives. Unlike other police stations in Kolkata, Sarsuna Police Station has ample space. Interestingly, as part of the green initiatives, we planned to install solar power. The Zonal Training Office of Life Insurance Corporation of India (LIC) is near the Sarsuna Police Station. We came to know that they sponsor projects in schools and other institutions. But as far as police stations are concerned, there aren’t too many instances. Once we approached them, they agreed to sponsor the solar project and on 11th November last year, two solar plants were installed with capacities of two kilowatts each.”

In case of local transportation for



beat patrolling, the Sarsuna Police Station was one of the first police stations to introduce e-cycles in a true environment-friendly perspective. One e-cycle was sponsored by the HDFC Bank whereas the other one was outsourced. This has indeed been a game-changer looking into the entire police force as the department is transitioning itself to eco-friendly steps for policing. The malkhana of the Sarsuna Police Station deserves special mention. Not only are there neatly crafted wooden boxes but also QR codes attached to them. Thus the police officials don't need to open the box, just scanning the QR code serves the purpose. Adequate pest control has been quite useful in the true sense of the term.

The Sarsuna Police Station also has a stylish cafeteria, run by the police personnel only. It has got a nice library where the visitors can have good leisure. In the case of gardening as well, this police station has been way ahead of the most. With a sophisticated environment-friendly approach, the whole campus is green and credit goes to the police personnel

for the timely maintenance and care. Waterlogging in the rainy season is indeed a matter of serious concern but will be resolved with further drainage work on part of the municipal authorities.

In the case of traditional policing, house visits of the women police personnel have been very effective. House visit has innovated traditional beat patrolling. Already more than 8,000 houses have been covered. Added to that, recorded as well as instant miking has helped to prevent cybercrime. Thankfully, due to constant campaigns on part of the Sarsuna Police Station, this locality has seen a lesser number of cases of bank fraud and other crimes. The Sarsuna Police Station is also working closely with the schools for awareness campaigns so that information is disseminated till the lower level in the best interests of the society. As this area is not categorically a business hub, crime concerning monetary transactions is rare. Dacoity and burglary are negligible as well. Cases of house theft and petty thefts are often registered, but in most cases, culprits are caught in no time.

The Sarsuna Police Station has been very compassionate in the social aspect as well. In the words of OC Siddhartha Chatterjee, "We have been very particular about preventing suicides which has been on the higher side in the post-Covid scenario. The Police Station is closely working with the NGOs. In fact, on behalf of the Police Station, we keep in touch with individuals where suicide attempts have been foiled. I want to mention two specific cases. A resident of Sarsuna who bought a new car and was a bar singer in the Esplanade area, tried to commit suicide after losing his job in the Covid. With timely vital inputs from his family, we saved him and presently he is recovering. We rescued a 14-year-old boy from a mishap. He was counselled thoroughly. Presently he is making drones and going ahead in technical innovations, making all of us proud."

Moreover, the Sarsuna Police Station has transgender toilets, portraying the gender neutral mindset and ethos of the Kolkata Police.



Cybercrime Investigation

What Every Officer Should Know

Some golden rules to start with.

1. Locard's Exchange Principle:

Paul L. Kirk expressed the principle as follows:

"Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him. Not only his fingerprints or his footprints, but his hair, the fibres from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects. All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment. It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value."

Dr. Edmond Locard, a pioneer in forensic science had formulated the basic principle of forensic science as: "Every contact leaves a trace".

The principle is sometimes stated as "Every contact leaves a trace", and applies to contact between individuals as well as between individuals and a physical environment. The above golden theory still holds good in case of cyber-crime investigation, the only difference is that here the physical world is replaced by the virtual world.

The amended section of Indian Evidence Act: section 3 says as follows:

2. As per Evidence Act, "Evidence" – "Evidence" means and includes –

(1) All statements which the Court permits or requires to be made

before it by witnesses, in relation to matters of fact under inquiry;

such statements are called oral evidence;

(2) All document including electronic records produced for the inspection of the Court, such documents are called documentary evidence;

3. Section 4 of the Information Technology Act, 2000 recognises information in electronic form for any laws in the following ways:

Legal Recognition of Electronic Records –Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is -

(a) Rendered or made available in an electronic form; and

(b) accessible so as to be usable for a subsequent reference.

4. E-Form Evidence:

Section 79A of the Information Technology Act is providing the concept of E-Form Evidence in the following ways:

Explanation–For the purposes of this section, “electronic form evidence” means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines.

5. Section 59 of Indian Evidence Act says:

Proof of facts by oral evidence. — All facts, except the contents of documents or electronic records, may be proved by oral evidence.

6. Section 65A of Indian Evidence Act says:



Special provisions as to evidence relating to electronic record: The contents of electronic records may be proved in accordance with the provisions of section 65B.

7. Section 65B of Evidence Act:

Under Section 65B(4) of the Evidence Act, if it is desired to give a statement in any proceedings pertaining to an electronic record, it is permissible provided the following conditions are satisfied:

(a) There must be a certificate which identifies the electronic record containing the statement;

(b) The certificate must describe the manner in which the electronic record was produced;

(c) The certificate must furnish the particulars of the device involved in the production of that record;

(d) The certificate must deal with the applicable conditions mentioned under Section 65B(2) of the Evidence Act; and

(e) The certificate must be signed by a person occupying a responsible official position in relation to the operation of the relevant device.

8. A judge also presides to see that a guilty man does not escape.

9. If a case is proved too perfectly, it is argued that it is artificial.

10. The maxim falsus in uno falsus in omnibus has no application in India and the witnesses cannot be branded as liars.

11. Investigation officer is not bound to record everything in the statement u/s 161 Cr.P.C.: F.I.R. and the statement recorded under section 161, Cr.P.C. are not encyclopaedia to give each and every minute details which had come into light during the deposition in the court. Sometimes witnesses do not think it proper to get it mentioned in the F.I.R. or in their statements recorded under section 161, Cr.P.C. but it does not mean that the facts do not exist.” (Dharmendra Singh and etc. v.



State of U.P., 1998 cri lj 2064)

12. The reliability of digital evidence:

in US v. Bonallo, (858 f. 2d 1427 – 1988 court of appeals, 9th 2002) a US court ruled that “the fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness”.

13. Last seen together and last resided together may also be electronically proved.

14. Conduct of the accused prior and after the incident may also be electronically proved.

14. Frye vs. United States, 293 F. 1013: Admissibility of Scientific Evidence: Expert opinion based on scientific technique is admissible only where the technique is generally accepted as reliable in the relevant scientific community.

15. Justice Stephen Breyer of the US Supreme Court ---- “Science in the Courtroom”, “In this age of science, science should expect to find a warm welcome, perhaps a permanent home, in our courtrooms... Our decisions should reflect a proper scientific and technical understanding so that the law can respond to the needs of the public.”

16. In Daubert Merrel Dow Pharmaceuticals Inc, the American Supreme Court -- “...there are important differences between the quest for truth in the courtroom and the quest for truth in the laboratory. Scientific conclusions are subject to perpetual revision. Law, on the other hand, must resolve disputes finally and quickly.” Replied by our Hon’ble Supreme Court in A.P. Pollution Control Board vs. Prof M.V. Nayudu.

17. In State of Maharashtra vs. Praful B. Desai (AIR 2003 SC 2053) the Hon’ble Supreme Court has observed that advancement in science and technology has also helped the process of law in administration of Justice.

18. In Sharat Babu Digumarti versus Govt. of NCT of Delhi, Hon’ble Supreme Court of India observed,

“Once the special provisions having the overriding effect do cover a criminal act and the offender, he gets out of the net of the IPC and in this case, Section 292. It is apt to note here that electronic forms of transmission are covered by the IT Act, which is a special law. It is a settled position in law that a special law shall prevail over the

general and prior laws. When the Act in various provisions deals with obscenity in electronic form, it covers the offence under Section 292 IPC. “

19. The landmark verdict on electronic evidence: Whether Certificate u/s 65B is mandatory? Latest Judgement by the Hon’ble Supreme Court of India. Every Learned Advocates, Investigation officers and common people must read this judgement.

To settle the two different interpretations between Anvar P.V. vs. P.K. Basheer & Ors. (2014) 10 SCC 473 and Shafhi Mohammad v. State of Himachal Pradesh (2018) 2 SCC 801, the matter was referred to the larger Bench of Hon’ble Supreme Court of India. We all were waiting for the verdict to come which would rest in peace the two completely different approaches of interpretation of “may be” clause in section 65A that is whether statement u/s 65B of Indian Evidence Act is mandatory or not and this Judgement (Arjun Panditrao Khotkar versus Kailash Kushanrao Gorantyal And Ors) solves many controversies regarding presentation, relevancy and admissibility of electronics evidence in Court room. In the following are the gist of this recent landmark judgement:

i) The certificate under Section 65B(4) is unnecessary if the original document itself is produced. If the owner proves a laptop, computer, computer tablet or a mobile phone owned or operated by him, bringing the same in the witness-box, on which the original information is first stored, the requirement of the statement or the certificate u/s 65B(4) is unnecessary.

ii) On the other hand, where the computer is part of a computer system or computer network and bringing the said system or network

before the court is impossible then providing the information contained in such electronic record can only be in accordance with section 65B(1) along with requisite certificate u/s 65B(4) of Evidence Act. Hence, in that situation the clarification made in para 24 of Anvar P.V. Basheer does not require to be revisited.

iv) The direction issue in para 62 of Arjun Panditrao Khotkar versus Kailash Kushanrao Gorantyal and Ors. judgement shall hereafter be followed by the court dealing with electronics evidence till rules and directions u/s 67C of I.T. Act and data retention conditions are formulated for compliance by telecom and internet service providers. In para 62, general directions are issued to cellular and internet service providing companies to maintain CDRs and other relevant records for the concerned periods in tune with section 39 of evidence act in a segregated and secure manner if a particular CDR or other records is seized during investigation in the said period. Concerned parties can then summon such records at the stage of defence evidence or if such data is required to cross examine a particular witness. The above direction in criminal trials be applicable till appropriate directions are issued under various relevant terms of the applicable license or u/s 67C of I.T. Act.

Penetration of Virtual World in Today's World:

India is heading for being the largest internet user in the world. As per Press Information Bureau, Government of India statistics in 2021, we find the following statistics:

The Users of various significant social medias: -

- WhatsApp users: 53 Crore
- YouTube users: 44.8 Crore



- Facebook users: 41 Crore
- Instagram users: 21 Crore
- Twitter users: 1.75 Crore

In our everyday life we are more prominent in the virtual world rather than in the physical world and hence the proportion of Cyber crimes or use of electronic forms of evidence have increased manifold.

Investigation and Traceability Path: Followings are the important steps in investigation with respect to a cyber crime cases:

Traceability of fraudsters can be expressed in four independent steps.

I. First, one determines the IP address to be traced from the URL available after asking through the domain name.

II. Second, one establishes which ISP has been allocated the IP address.

III. Third, the ISP's technical records will indicate which user account was using the IP address at the relevant time.

IV. Fourth and finally, the ISP's administrative records will

establish the real-world" identity of the individual who was permitted to operate the account.

(For details one can watch at: <https://www.youtube.com/watch?v=vNjrkQDupE4>)

Challenges before a Cyber Crime Investigator:

- i) Encryption nightmare of LEA: Use of IMs by Terrorists
- ii) Dark web attack & Crypto Currency:
 - a) onion
 - b) @Signait
 - c) Ransomware
 - d) BTC
- iii) Growing use of Cloud & Cloud not forensics friendly.
- iv) Difficulties in transferring information by Intermediaries abroad.
- v) Use of VOIP Call and SIP

Harvard University Case: FBI agents tracked Harvard bomb threats: Details can be read at: <http://www.theverge.com/2013/12/18/5224130/fbi-agents-tracked-harvard-bomb-threats-across-tor>

What should cyber investigators



have or should do?

- Experimenting attitude.
 - Techno-legal knowledge acquisition:
 - Coding Knowledge
- 1) Any one language: May be Python & Java Script
 - 2) May be a member of Coding community
- Think from the mind of a defence lawyer.
 - Cannot and should not deal on the suspect device.
 - Document every step in the road map of the electronic evidence.
 - Take help of section 27 and 8 of IEA in case the tech-savvy accused is only aware of the modus and motive of tech-crime.
 - Knowledge of Penetration Testing process with the Kali Linux Distribution (<https://www.kali.org/>)
 - Be careful about section 72A, 43, 43A of ITA, 2000 and other

provisions of laws

- Must have specific NDA-Indemnity sort of Agreement
- For judicial matter: By appropriate authorities and specific search warrant:

Forensics analysis involves the following steps:

- Collection – search and seizing of digital evidence, and acquisition of data.
- Examination – applying techniques to identify and extract data.
- Analysis – Analysis by using data and resources with standard norms.
- Reporting – presenting the report.
- Computer Forensic Analysis consists of the followings:
 - o Storage Media Analysis
 - o Software Source Code Analysis.
 - o Network traffic and logs Analysis.

Cybercrimes are basically of three categories and they are:

Cybercrimes against Property –
Financial crimes – cheating on-line
– illegal funds transfer.

Cybercrimes against persons –
Online harassment, Cyber Stalking,
Obscenity.

Cybercrimes against Nations –
Cyber Terrorism – Damaging
critical information infrastructures.

Cyber Laws In India :

- a. Information Technology Act, 2000.
- b. Information Technology (Amendment Act), 2008.
- c. Rules under Information Technology Act.
- d. Some Amendments in Cr.P.C., Evidence Act and Indian Penal Code.

Some of the important provisions of Information Technology Act, 2000 as amended for proper investigation are as follows:

- ❖ Section 4(1) and 4(2) of Cr.P.C. provide the provisions of Cr.P.C. are equally applicable in cases relating to other offences which may include offences under the Information Technology Act. The following are the special provisions which are having overriding effect with Cr.P.C. in case of police investigation.
- ❖ Special Provisions in IT Act & ITA Act:
- ❖ Section 76: Confiscation
- ❖ Section 77A: Compounding of offences
- ❖ Section 77B: Offence of Three years bailable
- ❖ Section 78 :Investigation by Inspector and above
- ❖ Section 80: Power to enter, Search, arrest without warrant

any person who is reasonably suspected of committed or committing or about to commit any offence under this Act.

- ❖ Section 84A : Modes or methods for encryption
- ❖ Section 77: Compensation, penalties or confiscation not to interfere with other punishments.

How One Can Adjudge Jurisdiction in Cyber Crime Cases:

When a Cyber crime is reported apart from having Zero FIR concept, the following provisions of law play a very crucial role:

Section 75 of IT Act :

75. Act to apply for offence or contraventions committed outside India.-

(1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

(2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

Section 4 of IPC: Extension of Code to extra-territorial offences.- The provisions of this Code apply also to any offence committed by-

- (1) Any citizen of India in any place without and beyond India;
- (2) Any person on any ship or aircraft registered in India wherever it may be.
- (3) Any person in any place without and beyond India committing an offence targeting a computer resource located in India.]

Explanation- In this section.-

(a) The word “offence” includes every act committed outside India which, if committed in India, would be punishable under this Code.

(b) The expression ‘computer resource’ shall have the meaning assigned to it in clause (k) of sub-section (1) of section 2 of the Information Technology Act, 2000 (21 of 2000)]

Offences under IT Act, 2000 & ITA Act, 2008:

- Section 65 - Tampering with computer source documents
- Section 66. Computer Related Offences. - If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment.....
- Section 66B Punishment for dishonestly receiving stolen computer resources or communication devices.
- Section 66C Punishment for identity theft.
- Section 66D Punishment for cheating by personation by using computer resources.
- Section 66E Punishment for violation of privacy
- Section 66F Punishment for cyber terrorism.
- Section 67 Punishment for publishing or transmitting obscene material in electronic form.
- Section 67 A Punishment for publishing or transmitting of material containing
- Sexually explicit act, etc., in electronic form.
- Section 67 B Punishment for publishing or transmitting of material depicting
- Children in sexually explicit act, etc., in electronic form.
- Section 67 C Preservation and retention of information by intermediaries.
- Section 71 Misrepresentation to the Controller or the Certifying Authority.



- Section 72 Offence relating to Breach of Confidentiality and Privacy
- Section 72A Offence relating to disclosure information in breach of lawful contract
- Section 73 Publishing Digital Signature Certificate false in certain particulars.
- Section 74 Offence relating to Publication of fraudulent purpose
- Section 84B Abetment of offence
- Section 84C Attempt to commit offences

Cybercrimes against nations - Cyber Terrorism - Damaging critical information infrastructures:

CYBERTERRORISM: Cyber terrorism is the convergence of terrorism and cyberspace. Section 66F of ITA, 2008 provides Definition and Punishment of Cyber terrorism being Life Imprisonment.

Section 70 : Any person who secures access or attempts to secure access to a protected system will be punishable up to 10 years.

National Cyber Security Policy 2013 to protect 'Critical Information Infrastructure' : 24 x 7 hours protection is required to safeguard the nation.

Cyber Pornography & Obscenity:

Huge amount of data in the internet are related to obscene and pornographic data: The principles guiding the obscenity can be as follows:

a. Hicklin' test of obscenity: "I think the test of obscenity is this, whether the tendency of the matter charged as obscenity is to deprave and corrupt those whose minds are open to such immoral influences, and into whose hands a publication of this sort may fall.



b. Miller Test: The Miller test was developed in the 1973 case Miller vs. It has three parts:

- Whether "the average person, applying contemporary standards", would find that the work, taken as a whole, appeals to the prurient interest,
- Whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by applicable state law,
- Whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value.

Apart from Information Technology Act, 2000 Other Indian Laws That Deal with Pornography:

- i) Indecent Representation of Women (Prohibition) Act.
- ii) Indian Penal Code Section 293. Sale, Etc., Of Obscene Objects to Young Person 292. Sale, Etc., Of Obscene Books, Etc.
- iii) The Protection of Children From Sexual Offences Act, 2012.

Lawful and Unlawful Interception: Following provisions of the Information Technology Act provide laws of interception which every Investigating officer

should know, because unlawful interception is a nightmare for every law enforcement agency today.

i) Section 69 of Information Technology Act: Power to issue directions for interception or monitoring or decryption of any information through any computer resource.

ii) Section 69A of Information Technology Act: Power to issue directions for blocking for public access of any information through any computer resource.

iii) Section 69B of Information Technology Act: Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security.

In every case when one investigating officer asks for a CDR. SDR, IPDR, IP Log etc., he should know the following observation:

Maharashtra v. Bharat Shanti Lal Shah & others

In State of Maharashtra v. Bharat Shanti Lal Shah & others ((2008) 13 SCC 5) the Hon'ble Court observed "The interpretation of conversation though constitutes an invasion of

an individual right to privacy but the said right can be curtailed in accordance with procedure validly established by law. Thus what the Court is required to see is that the procedure itself must be fair, just and reasonable and non-arbitrary, fanciful or oppressive."

But following relaxation is also available:

A. Relevant part of landmark judgement on Evidentiary Value of intercepted data: Dharambir Khattar vs Union Of India & Another on 21 November, 2012 by Hon'ble High Court Of Delhi. "Therefore, without going into the issue of whether there was non-compliance of the provisions of Section 5(2) or of Rule 419-A, it is clear that even if there was, in fact, no compliance, the evidence gathered thereupon would still be admissible. This is the clear position settled by the Supreme Court and, therefore, no further question of law arises on this aspect of the matter."

B. Section 84 of Information

Technology Act: Protection of Action taken in Good Faith.-No suit, prosecution or other legal proceeding shall lie against the Central Government, the State Government, the Controller or any person acting on behalf of him, the Chairperson, Members, Adjudicating Officers and the staff of the Cyber Appellate Tribunal for anything which is in good faith done or intended to be done in pursuance of this Act or any rule, regulation or order made there under.

When an Investigation officer deals with Electronic Evidence, He should keep in his mind the following:

- A. Electronic evidence is information and data of investigative value that is stored on or transmitted by an electronic device
- B. Electronic evidence is, by its very nature, fragile.
- C. It can be altered, damaged, or destroyed by improper handling

or improper examination. For this reason, special precautions should be taken to document, collect, preserve, and examine this type of evidence.

- D. The nature of electronic evidence is such that it poses special challenges for its admissibility in court.
- E. Chain-of-custody is the collection, preservation and analysis of evidence for the purpose of establishing authenticity and reliability of evidence.

CRYPTOCURRENCY:

Bitcoin or cryptocurrency is a topic that has sparked our curiosity. Indeed, today many people want to invest in cryptocurrency or Bitcoin and with the rise of home-based stock trading via different mobile apps, many will be unable to resist the seduction of various cryptocurrencies.

The price of a Bitcoin peaked around Rs. 42 lakh in early May 2021, but





dropped below Rs. 25 lakh, a few days later after the publishing of news on the worldwide market. Now the question is, since Bitcoin is a digital currency or asset that does not follow the centralized currency system, there is no government agency to oversee the fluctuations and mobility of Bitcoin or other cryptocurrencies and its outcome.

Innovation of Bitcoin – Satoshi Nakamoto White Paper – Satoshi Nakamoto identity

If we go back a little bit, we can see that there was an economic recession all over the world from 2007 to 2009, and about the same time in 2009, a white-paper titled “Bitcoin: A Peer-to-Peer Electronic Cash System” was released on the bitcoin.org website. In the front page of a nine-page white paper written by Satoshi Nakamoto, he says Bitcoin is “A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.”

Although this nine-page white paper is quite complex, Satoshi Nakamoto describes on the second page, “We define an electronic

coin as a chain digital signature.” In the eighth page under heading “Conclusion”, he wrote “We have proposed a system for electronic transactions without relying on trust”.

How do law enforcement agencies investigate Bitcoin ? - Why do hackers use Bitcoin?

Another aspect to consider is how the investigating officials can gather money trail when the crime has been committed using Bitcoin. In a nutshell, Bitcoin incorporates features that use encryption and digital signatures to protect the Bitcoin network’s security, thus it is a part of the virtual world but has nothing to do with its physical existence and due to which it cannot be traced out. We have seen the use of Bitcoin in many heinous types of crimes starting from narcotic drugs sale to large-scale ransomware.

Now let us see the positions of law on Bitcoin or different types of cryptocurrencies.

Is it legal to invest in Bitcoin or cryptocurrency? - Should you invest in cryptocurrency?

This is a question that occurs in many people’s minds nowadays.

Let’s take a look at the scenario. After the invention of Bitcoin, several countries around the world outright banned it; nevertheless, certain countries have a liberal outlook. There are even countries who have come up with laws defining cryptocurrencies, namely Japan, Malta, Canada, Bahamas, Estonia, Latvia, Israel, Mexico, Austria, Czech Republic, Germany, Luxembourg, Slovakia, the European Union and the United Kingdom.

Whether Bitcoin is legal in India? RBI circular on cryptocurrency - RBI on cryptocurrency - Supreme Court on cryptocurrency

Let us see it chronologically....

24-12-2013 : The Reserve Bank of India has issued a warning to users, holders, and traders of “Decentralised Digital Currency” or “Virtual Currency,” such as Bitcoins, regarding the potential financial, operational, legal, customer protection, and security risks they are taking.

1-2-2017: The Reserve Bank of India has not granted any business or firm a licence or authorization to operate or deal in Bitcoin or any other virtual currency. As a result, anyone interacting with Virtual Currencies, whether as a user, holder, investor, trader, or otherwise, does so at their own risk.

5-4-2018: Consumer protection, market integrity, and money laundering are among the problems raised by virtual currencies, often known as crypto-currency and crypto assets.

6-4-2018: The RBI’s regulated firms like Commercial Payment Banks, Small Finance Banks, NBFCs are prohibited from dealing in virtual currencies or providing services to assist anyone in dealing with or settling virtual currencies.

Regulated entities that already supply such services must end the arrangement within three months of this circular's publication.

20-03-2020: A case was then filed in the Hon'ble Supreme Court challenging the Circular known as Internet and Mobile Association of India v. Reserve Bank of India, Writ Petition (Civil) No.528 of 2018, in which the Hon'ble Supreme Court set aside the aforementioned RBI circular.

On 31-05-2021: The Reserve bank of India informed that, in view of the order of the Hon'ble Supreme Court, the prohibition circular over Virtual Currencies is no longer effective from the date of the Supreme Court judgement. Banks, as well as other entities may, however, continue to carry out customer due diligence processes in line with regulations governing standards.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, introduced on 25th February in India :

IT Rules 2021 is very useful and crucial and rather solves the age old issue of the international significant social media to cooperate with the Investigating agencies apart from other issues it covers.

In one recent case i.e. Facebook Inc. versus Union of India & ORS., the issue relating to how and in what manner the intermediaries should provide information including the names of the originators of any message/content/information shared on the platforms run by these intermediaries and decryption of end-to-end encrypted chat-messengers who are to provide data in time of investigation etc. were raised and the question of any Rule to that effect was also discussed.

Some salient features of IT Rules 2021:

➤ 72 Hrs. Compliance to provide data to Government Agencies: Intermediary shall, as soon as possible, but not later than seventy-two hours of the receipt of an order, provide information under its control or possession, or assistance to Government agency.

➤ 24 Hrs. to remove obscene materials etc.: As per the Section 3(2)(b) of this Rule, the intermediary shall, within twenty-four hours from the receipt of a complaint made by an individual or any person on his behalf under this sub-rule, in relation to any content which is prima facie in the nature of any material which exposes the private area of such individual, shows such individual in full or partial nudity or shows or depicts such individual in any sexual act or conduct, or is in the nature of impersonation in an electronic form, including artificially morphed images of such individual, take all reasonable and practicable measures to remove or disable access to such content which is hosted, stored, published or transmitted by it.

➤ As per Rule 3(1) : What should not be published etc.: As per Rule 3(1) the intermediary shall not host, display, upload, modify, publish, transmit, store, update or share any information that,

o belongs to another person and to which the user does not have any right;

o is defamatory, obscene, pornographic, paedophilic, invasive of another's privacy including bodily privacy, insulting or harassing on the basis of gender, libellous, racially or ethnically objectionable, relating or encouraging money laundering or gambling, or otherwise inconsistent with or contrary to the laws in force;

o is harmful to child;

o infringes any patent, trademark, copyright or other proprietary rights;

o violates any law for the time being in force;

o deceives or misleads the addressee about the origin of the message or knowingly and intentionally communicates any information which is patently false or misleading in nature but may reasonably be perceived as a fact;

o impersonates another person;

o threatens the unity, integrity, defence, security or sovereignty of India, friendly relations with foreign States, or public order, or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting other nation;

o contains software virus or any other computer code, file or program designed to interrupt, destroy or limit the functionality of any computer resource;

o is patently false and untrue, and is written or published in any form, with the intent to mislead or harass a person, entity or agency for financial gain or to cause any injury to any person;

➤ It is further to be mentioned that as per the Rule 3 of IT Rules 2021, intermediaries have to preserve Evidence or retain Data for 180 Days.

➤ In this Rule the social media has been divided into two parts, they are:

1) Significant social media intermediary.

2) Social media intermediary.

➤ One Significant social media intermediary should have: -



- a. Chief Compliance Officer,
- b. A nodal contact person needs to be appointed 24x7 to coordinate with law enforcement agencies.
- c. A Resident Grievance Officer.

➤ **Identification of the First Originator for messaging Apps like WhatsApp etc.:**

As stated in the Rule 4(2), a significant social media intermediary providing services primarily in the nature of messaging shall enable the identification of the first originator of the information on its computer resource as may be required by a judicial order passed by a court of competent jurisdiction or an order passed by the Competent Authority under section 69 of the Information Technology (Procedure and Safeguards for interception, monitoring and decryption of information) Rules, 2009, which shall be supported with a copy of such information in electronic form.

➤ **“Safe-Harbour Protections” under Section 79 of the IT Act and Proviso Clauses:** There is a lot of debate with respect to instant messenger like WhatsApp etc. whether the privacy they offer by way of end-to-end encryption will be violated. But if one studies the proviso clauses of this 4(2) of this

Rule, it will be clear that nothing of that sort has been there and on the contrary the messages or chat cannot be intercepted or to be taken.

➤ **Consequence of Non-Compliance –Rule 7 specifies the consequences of Non-observance of Rules:** Where an intermediary fails to observe these rules, the provisions of sub-section (1) of section 79 of the Act shall not be applicable to such intermediary and the intermediary shall be liable for punishment under any law for the time being in force including the provisions of the Act and the Indian Penal Code.

How to deal with electronic evidence:

In today’s world in proving any case electronic evidence can play an important role.

The recent judgements which are worth mentioning in India are as follows: “In Ziyauddin Burhanuddin Bukhariv. Brijmohan Ramdass Mehra [Ziyauddin Burhanuddin Bukhari v. Brijmohan Ramdass Mehra, (1976) 2 SCC 17], this Court noted that new techniques and devices are the order of the day. Audio and video tape technology has emerged as a powerful medium through which first-hand information can

be gathered and can be crucial evidence.”

The most important criticism of digital evidence is that digital evidence can be easily altered.

However, in US v. Bonallo (858 F. 2d 1427 - 1988 - Court of Appeals, 9th 2002) a US court ruled that “the fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness”.

As discussed above, out of all the qualities of Electronic Evidence Relevancy and Admissibility are two most important. An investigator should know or ought to know what is relevant for his case to collect as evidence, be it direct or documentary. In order to prove the admissibility, I have already discussed the details of Section 65B of Indian Evidence Act. Following are some formats which one can follow to draft their required statement as per their facts and figures.

Error! Filename not specified.

Error! Filename not specified.

Error! Filename not specified.

(https://en.wikipedia.org/wiki/Locard%27s_exchange_principle)

Sources:<https://pib.gov.in/PressReleaseDetail.aspx?PRID=1700749>

https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf •



In this modern world, while we enjoy the perks of modern online banking and digital platforms, we also need to be aware of the increased risks that come along with the use of platforms like Netbanking and Mobile banking and mobile payment apps. Fraudsters continuously try to steal confidential data - Customer ID, IPIN, OTP, account number, etc. through website pop-ups, emails, calls, and SMS messages.

Below are some of the modus

operandi and some advice on how you can protect your financial data.

Phishing

Phishing is a type of fraud that involves stealing personal information such as Customer ID, IPIN, Credit/Debit Card number, Card expiry date, CVV number, etc. through emails, that appear to be from a legitimate source, say HDFC Bank. Nowadays, phishers also use phones (voice phishing) and SMS (Smishing).

How do fraudsters operate?

- Fraudsters pose as bank officials and send out emails with an attached link, urging customers to verify or update your account data.
- Clicking on the link takes the customer to a fake website with a web form to fill in their personal information.
- Information so acquired is then used to conduct fraudulent transactions on the customer's account.

How to identify fake Phishing website:

- Verify the URL of the webpage. The 's' at the end of 'https://' stands for 'secure' - meaning the page is secured with an encryption. Most fake web addresses start with 'http://'. Beware of such websites!
- Check the Padlock symbol. This depicts the existence of a security certificate, also called the digital certificate for that website.
- Ensure the authenticity of the website by verifying its digital certificate by clicking on the padlock symbol at the top left of your browser window.

How to protect yourself from Phishing:

Dos

- Always check the web address carefully. For example the Netbanking address of HDFC Bank Ltd is <https://netbanking.hdfcbank.com>
- Always check the web address carefully.
- Always type the website address in your web browser when logging in.
- Always check for the Padlock icon at the upper or bottom right corner of the web page to be 'On'.
- Install the latest anti-virus/ security patches on your computer or mobile phones.
- Always use non-admin user ID for routine work on your computer.

Don'ts

- DO NOT click on any suspicious link in your email.

- DO NOT provide any confidential information via email, even if the request seems to be from authorities like the Income Tax Department, Visa or MasterCard etc.
- DO NOT open unexpected email attachments or instant message download links.
- DO NOT access Netbanking or make payments using your Credit/Debit Card from computers in public places like cyber cafés, public WIFI .

Vishing

Vishing is one such attempt where fraudsters try to seek your personal information like Customer ID, Netbanking password, ATM PIN, OTP, Card expiry date, CVV etc. through a phone call

How do fraudsters operate?

- A fraudster poses as an employee from the bank or a Government / Financial institution and asks customers for their personal information.
- They cite varied reasons as to why they need this information. For e.g. reactivation of account, KYC , en-cash of reward points, sending a new card etc.
- These details thus obtained are then used to conduct fraudulent activities/ transactions on the customer's account without their knowledge.

How to protect yourself from Vishing:

- Never share any personal information like Customer ID, ATM PIN, OTP etc. over the phone, SMS or email.
- If in doubt, call the Phone Banking number, as mentioned

on the reverse side of your card or on www.hdfcbank.com

Smishing

Smishing is a type of fraud that uses mobile phone text messages to lure victims into calling back on a fraudulent phone number, visiting fraudulent websites or downloading malicious content via phone or web.

How do fraudsters operate?

- Fraudsters send SMS intimating customers of prize money, lottery, job offers etc. and requesting them to share their card or account credentials.
- The customers follow instructions to visit a website, call a phone number or download malicious content.
- Details thus shared with the person who initiated the SMS are then used to conduct fraudulent transactions on the customer's account, causing them financial loss.

How to protect yourself from fraud:

- Never share your personal information or financial information via SMS, call or email.
- Do not follow the instructions as mentioned in SMS sent from untrusted sources, delete such SMS instantly.
- If you receive a message asking for personal information, call the Phone Banking no. found on the reverse side of your card or on www.hdfcbank.com.

UPI Frauds

During the ongoing COVID- 19 crisis that has forced people to

stay at home, online payments have been preferred by many as they can pay for their purchases right from the comfort of their homes. Fraudsters have made best use of this situation to deceive people and make profit for themselves.

UPI frauds via request money (Collect request) feature: Fraudsters pose themselves as genuine buyers and convince the customer to accept the collect request under the pretext of making payments. Fraudsters share the QR code/ pay internet link by which they can receive money. Ignorantly a customer authorises these “Pay” transactions and funds are debited from the customer’s account itself.

UPI fraud via cashback scam: In order to lure you into cashback offers, fraudsters might call you in the disguise of a bank’s or retail store’s customer care executive and say that you have won some cashback and ask you to accept it via any UPI app. Once you fall for their attempt, you will get the message of the mentioned amount on your UPI app. Now waiting to get this cashback, you might enter your UPI PIN, which will transfer money to the caller’s account.

UPI frauds via Remote Screen Mirroring tools:

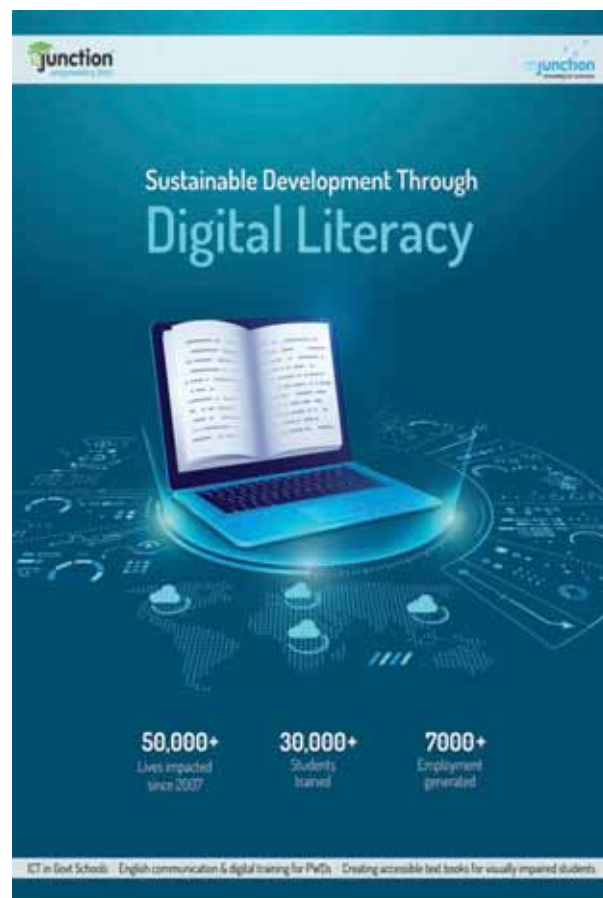
- The fraudsters get hold of your contact number and call the unsuspecting customer posing as a representative of a bank or any other financial institution.
- Once the fraudster has convinced the victim, they proceed to ask to download an application such as AnyDesk, Screen share, Team viewer, etc on your phone.
- The fraudster will then ask the victim for a 9-digit OTP, which is generated on their phone. As soon as the victim reveals the code, the hacker will also ask to grant permission for their phone.
- When the app acquires all the permission required, the fraudster starts to take full control of the victim’s phone without their knowledge. After getting full access to their phone a hacker steals passwords and begins transacting with the victim’s UPI account.

UPI fraud prevention:

- Government agencies, banks and other financial institutions never ask for financial information such as OTP, Password, UPI PIN/MPIN, etc via SMS/ Email/Phone.

- Do not make online payments without cross verifying the source. Be alert to transfer requests on UPI as fraudsters are taking advantage of the request money feature on UPI app.
- Do not install remote access apps, to share access to your mobile phone to third parties.
- Do not share your confidential banking details & personal information with anyone.

Stay alert and keep your confidential data safe from fraudsters.



Kolkata Police Served Senior Citizens Well During COVID Pandemic

Soven Banerjee,

Assistant Commissioner of Police, Kolkata Police

During the COVID-19 pandemic, the social isolation of senior citizens became more and more conspicuous.

It is not only about the dependence on daily (financial and physical) and regular needs on others, but abuse of senior citizens has become a global public health issue, which is detrimental to their mental as well as physical health.

In India, half of the senior citizens survive by virtue of dependence on others. However, only 20% are partially dependent on financial needs. Around 85% of the senior citizens have to rely on others for daily needs (NSSO, 52 rounds).

According to a Age Well Foundation report, around 71% of senior citizens have faced exploitation during the lockdown phase.

The survey shows a sharp deteriorating interpersonal relation as the main reason behind the atrocities against senior citizens in the family.

In more than 56% of such cases, family members, (son: 43.8%, daughter-in-law: 27.8%, daughter: 14.2%), friends, and caregivers are the main accused. According to the survey report of Help Age India, emotional abuse amounted to 60.1% of cases, followed by financial and physical abuse.

The report also pointed out that 20.5% of senior citizens wanted someone to just be with them and 35.7% wanted someone to call them and talk.

During the lockdown, more females were abused (22.34%) than males (16.95%) as reported by the India Journal of Gerontology.

A total of 13,126 senior citizens committed suicide and in 33.6% of cases, family issues remained the key parameter (NCRB 2020). The Kolkata Police made it a point to ensure that social isolation did not hurt their mental health leading them into mental depression.

As senior citizens are weak, they are an easy target for criminals. The NCRB 2020 data shows that in 19 cities of the country, there were 4,029 cases of crime against senior citizens.

In the case of crime against senior citizens, the Kolkata Police has filed charge-sheets in a maximum number of cases i.e. more than 96% (NCRB 2020).

In the entire COVID phase, among the total casualties around the world, 63% belonged to the senior citizens category.

In India too, the situation wasn't different. No doubt, old age and comorbid conditions played their part in it. As per the data shared by the Health and Family Welfare

Department, GOI, 86% of the senior citizens who passed away due to the COVID, suffered from heart and lung diseases, long term kidney ailments, high blood pressure and other cardiac complications.

An interesting insight has come out that those who have a history of heart and lung diseases or diabetes or have been suffering from cancer are more susceptible to viral infections.

As the comorbid condition is common among senior citizens, it is indeed challenging to safeguard them against COVID. As per data released by the Government of WB, among the COVID casualties in the state, 64.2% were senior citizens.

The Kolkata Police remains committed to the needs of citizens without making any distinction. Apart from traditional policing involving regular maintenance of law and order in the city, the police force has been catering to the needs of the lesser privileged, deprived and weaker sections of society.

The way Kolkata Police stood by the senior citizens of the city along with the Pronam Project is indeed exemplary. Senior citizens living alone/couples in Kolkata can become a member of Pronam. For the needs of senior citizens, there is a dedicated control room which works 24x7. Not only for health needs, even for physical needs,



the Kolkata Police is ready to help elderly people.

A dedicated team at every police station has been formed to look after the well being of Pronam members. The liaison team visits the house of Pronam members once in a month and calls them on the telephone fortnightly. Kolkata Police organises various cultural, social, entertainment events at regular intervals for Pronam members to remove loneliness.

During the lock-down phase, 1,752 members contacted the Pronam control room for their daily needs, 184 rang up for health issues whereas 372 of them called for medicine, mask and sanitizers, 68 persons called for cooking gas and many others for grocery, nurses, caregivers, electricians, plumbers and all for daily needs, apart from that uncountable members called to their local police liaison officers for not only their need but to say “Amra Bhaloi Achi, Tomra Khub Khub Sabdhane Theko”.

These are only facts and figures of service provided for Pronam members, but actually all 78 Police Station, 25 Traffic Guards and Police Clubs acted simultaneously during the lock-down period to supply dry rations, cooked foods, medicines, masks, sanitizers to the weaker sections across the length and breadth of the city.

Not only that, the Kolkata Police reached out to the senior citizens and motivated them through cultural performances at the housing complexes, on streets and also over a phone call.

Even the Commissioner of Police along with other senior officials of the Kolkata Police participated in various cultural programmes in the virtual format to motivate senior citizens and interacted with them regularly.

No doubt, social isolation is one of the grave issues among senior citizens in the public health domain.

Kolkata Police believes that senior citizens are strong pillars of human resources of the city who

are enriched with knowledge, experience and sharp insights.

Although many of them have retired, they are physically fine and mentally quite capable. In a conducive environment, they have the potential to play an active role in the socio-economic development of the society.

Kolkata Police will keep serving the senior citizens, as part of the family and have the highest regard and concern for them for the greatest good of society.

‘Say not the struggle availeth not.’ – After all, society prospers when every family enjoys active participation of the elderly members beyond sixty, achieving a splendid rapport without focussing on the differences.

Death is imperative but a life of togetherness can spell a unique socialisation and oneness. Law alone cannot ensure prosperity; it is a family’s social awareness and genuine concern for the aged that can bring about unbound joy and fulfilment. •

Coronavirus Impact on the Elders and the Exemplary Role of Kolkata Police



The Coronavirus pandemic took a heavy toll on elders in our country. Similar trends were observed in other countries also. As a consequence, older adults were identified as a group at risk, and strict government restrictions were imposed on them. This has caused concerns about their physical and mental health. There is a significant decrease in activity level, sleep quality and wellbeing during the COVID-19 pandemic. This implies that this group at risk requires attention of the state governments and healthcare officials.

Elderly people are one of the most vulnerable groups, not only physically or mentally but also socio-economically. As a Geriatric physician and a social activist, I would like to share my experience of being deeply involved with older people especially during the pandemic period.

There are two ways to discuss how the pandemic affected the elderly. Elderly people can be divided into two groups for the convenience of discussion, one is socio-economically backward and the other is affluent. While some problems are the same for the two sections, there are some problems that are completely different. But in a word, the elderly in two sections as a whole have been deeply affected by this pandemic.

In the socio-economically backward part, the elderly are already very weak financially, but in the pandemic, that financial weakness has increased a lot. As the whole family suffered a severe financial crisis, the elders in the family became more and more brittle and neglected in all aspects. In many cases, even older people have been forced to commit suicide because of this. Due to this financial crisis, most of

the elderly have been unable to eat even their daily meals and this has led to many malnutrition problems. Marginalized elders are already neglected on the health front and that neglect has increased a lot more during this pandemic. Many cases of corona infections have been reported even among this section.

Many of the older people of this section could not get the corona vaccine because of the shortage of people to take them to the vaccination centre. In many cases, their family members did not pay any attention to it. Most of the health centres could not provide any treatment to the elderly due to non-availability of healthcare staff other than those dedicated to corona at this time. Therefore, the elderly have not been able to get any treatment for their chronic diseases like Hypertension, Diabetes, Cardiac ailments, COPD etc and as a result of which they have become uncontrollable, leading to severe complications and even death. Different types of mental problems have also been noticed among the marginalized elders due to situational reasons. Many were suffering from mental depression. Due to both physical and mental stress, the working capacity of the marginalized elders has also decreased a lot, as a result of which they have become more brittle in the family. I have had the opportunity to look at these issues in terms of being directly involved in the treatment of the elderly in various marginalized places, especially in the Sundarban through my organization 'Banchbo'.

Now let's discuss the condition of affluent elders in the city of Kolkata during this pandemic. This pandemic taught us that no matter how much money we have, we need more manpower than money. During Corona's first lockdown period, even many

millionaire elderly were forced to starve because there was no storage of food in their house. Since most of the children of the elderly in the city live outside the city or abroad, their biggest concern was shortage of manpower. Even the elderly did not have enough people to bring them the basic necessities and medicines they needed at that time. The role of the Kolkata Police and various NGOs like 'Banchbo' at this time deserves considerable praise. I was myself involved in the home isolation treatment of many elderly Corona patients both in the first and second wave. The first and second waves of the Corona affected many elderly people in this category and also killed many. In many cases no one was found to take the elderly person to the hospital or to contact them after admission. In many cases their cremation was completed without the presence of their family members. A situation that is truly indescribable. And because of this uncertainty, older people have been forced to go through a lot of emotional or mental stress. It has also had a profound effect on physical health. Many are suffering from insomnia due to such anxiety and stress. The treatment of chronic diseases like Hypertension, Diabetes, COPD, Ischaemic Heart Disease, Alzheimer's, Parkinson's, Different Movement Disorders, Hypothyroidism etc. of these elderly people has been hampered due to not being able to see a regular doctor. Even because of that the diseases have remained very uncontrollable. Due to which the physical condition of many elderly people has been severely damaged and many have died due to this.

Although the practice of telemedicine has been introduced as a complementary measure, most of the elderly people have not been able to enjoy the benefits of this telemedicine except for a

fraction. No matter how educated they are, a large part of them are not yet technologically savvy, so this system of telemedicine has remained elusive to them. Although hesitant at first, most elderly people have already taken two doses of the Corona vaccine and many have taken even their booster dose. Many seniors have not been able to get the vaccine yet due to lack of people to take them to the vaccination centre. The bedridden elderly suffer the most. Although various NGOs, including 'Banchbo', 'Dignity Foundation', have sided with the elders in this regard, it is very limited compared to the demand. The government must pay enough attention to this issue. Due to being confined at home for a long time, the physical inactivity of most of the elderly has increased a lot. And it has affected the elderly both physically and mentally. This has led to increased reliance or dependency on other people, especially caregivers or maids.

The number of trained caregivers in the country is so low that the elderly are forced to take untrained maid's services. And by taking advantage of this opportunity, the Aya Centres have increased the rates, which is beyond the reach of many common elderly people. Because of such unskilled and untrained ayah's services, many unwanted incidents have happened and even many old people have died. The elders have also had to face many incidents of physical and mental abuses by maids.

This pandemic has severely damaged the mental health of older people. Many older people suffer from various mental health problems, including depression. This will be a big problem for doctors in the coming days. Various statistics say that this pandemic has led to an increase in various forms

of abuse and torture of elderly by the family members and others in the society. This is really a serious issue. It is imperative to take action immediately in this regard from all levels of society.

The government desperately needs to think about this as soon as possible and take some appropriate steps. There is a definite need for action, both in the short and long-term to minimize the negative effects of the digital divide during this pandemic, and to act to bridge the divide in the long term. Action by governments to increase access to technology and implement digital literacy programmes among elderly populations is absolutely necessary, especially going forward into an increasingly digital future.

In this case, more interested NGOs should be involved. Whenever the opportunity arises, I have repeatedly mentioned in discussions on various platforms that it is important to engage local clubs to ensure the safety of the elderly on a cluster basis. If necessary, some volunteer forces can be formed and in this case the government needs to provide financial help to the local clubs for the volunteers.

The role of the Kolkata Police and 'Pronam' in protecting the elderly is commendable, especially during the lockdown period and the way in which the Kolkata Police stood by the elders during the Corona pandemic is exemplary. The role of Kolkata Police in being with the elders in pandemic times is truly commendable and exemplary. Kolkata Police and its community wing are on the side of the city elders day and night for various needs ranging from providing food or dry rationing to supplying emergency medicines at the beginning of Corona pandemic. In this case, officers from every police station

of Kolkata Police starting from Lalbazar, the head office of Kolkata Police and top officials including the Commissioner of Police have looked directly at the situation and taken action immediately. Kolkata Police has implemented these works with the help of various NGOs including 'Banchbo'. During this time, the Kolkata Police launched a 24-hour helpline to help the elderly. Lots of senior citizens have benefited from this and the helpline number has been used to contact the senior citizens with their useful related organization or contacts and in many cases the police themselves have extended a helping hand. 'Pronam' Liaison Officers have maintained or still maintain regular contact with elder personnel, especially those who are alone in each police station. As a result of this role of the police, the elderly people had a peace of mind during this crisis time. This effort of the Kolkata Police has been praised on national channels like NDTV. During the lockdown, police officers from different police stations even gathered at different places in the area to sing songs to give emotional joy to the elders touching everyone's heart. This innovative effort of the Kolkata Police has been highly praised by all. Shortly after the newly appointed Commissioner of Police, Shri Vinit Goel, IPS, took over, six virtual meetings were organized by the Pronam of Kolkata Police with the elders of each division last January. The presence of elders in those meetings was very spontaneous and eye-catching. The meetings were attended by senior police officers and OCs of the different police stations and divisions, and also the honorable Kolkata Police Commissioner himself and the Additional Commissioner, Joint-Commissioners, to encourage the elders. Various cultural programmes have been organized

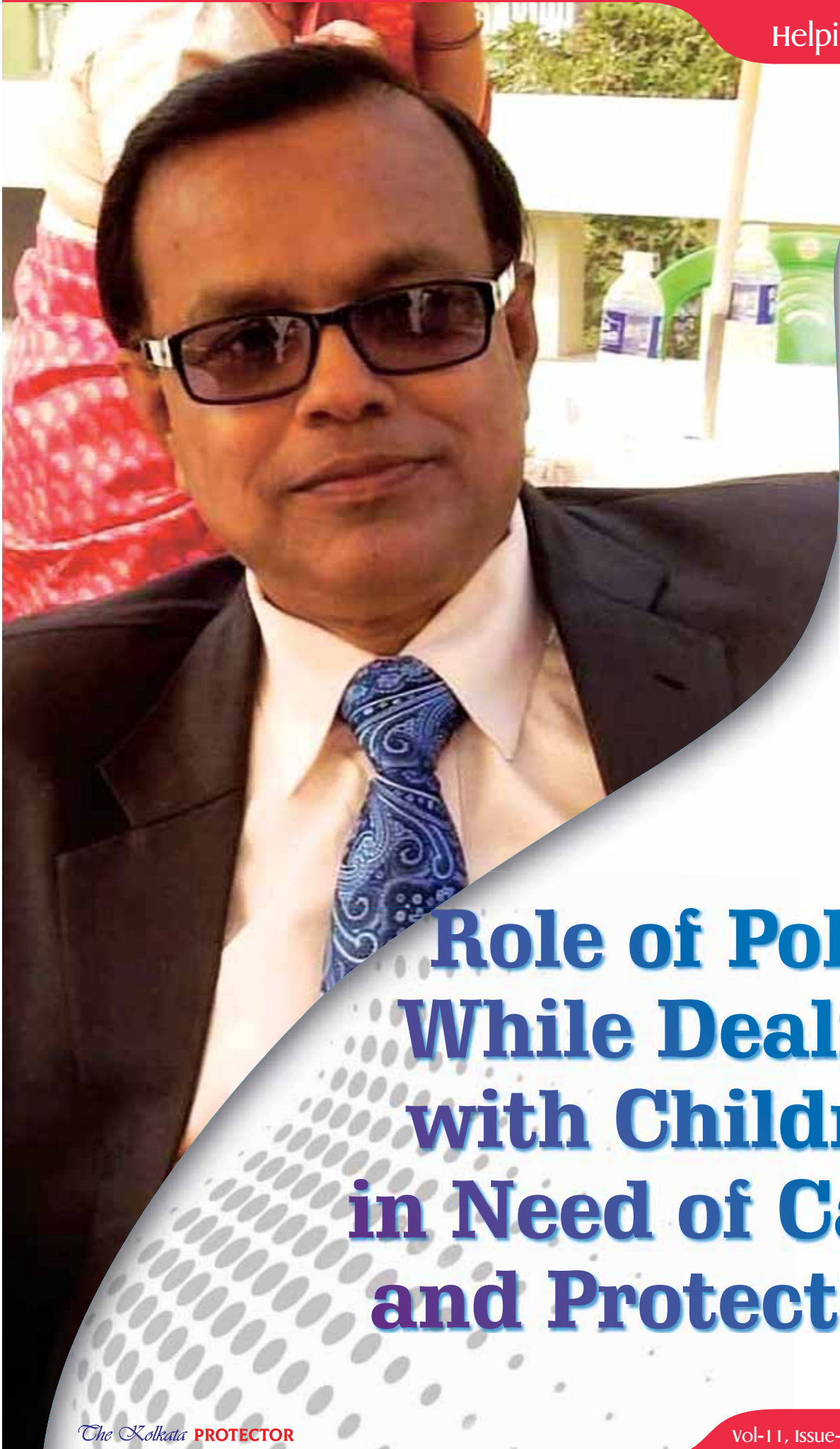
in these events to give peace of mind and pleasure to the elderly people during this turbulent time. Various well-known musicians and filmmakers including Mr. Arindam Sil, Mrs. Sriradha Bandopadhyay, Mrs. Iman Chakraborty from Kolkata were present on the occasion to encourage the elders. Former captain of the Indian cricket team and most popular iconic figure and one of our acquaintances Mr. Sourav Ganguly himself was present at one of the events which made the elders really happy. I personally attended these six episodes at the invitation of the Kolkata Police as a Guest speaker to talk about how the elderly can be mentally and physically fit. I myself have enjoyed and been enriched by attending these events. The role of the Kolkata Police in being by the side of the elders in making such various efforts is highly commendable. Our big salute to all the members of Kolkata Police for their noble work.

Unless everyone else, like the Kolkata Police, desperately needs to take such an initiative, we will not be able to provide the necessary respect and protection to our beloved elders. People from all walks of life as a whole have to come forward to keep the elders well in their second innings.

Let us all remember this -

"Nobody grows old merely by living a number of years. We grow old by deserting our ideals. Years may wrinkle the skin, but to give up enthusiasm wrinkles the soul."
- Samuel Ullman

Dr. Dhiresh Kumar Chowdhury
Geriatrician and Social Activist
Founder and President: Banchbo
(www.banchbongo.org)
Assistant Secretary: Geriatric Society of India, West Bengal Branch
Executive Member: Protect The Warriors.

A photograph of a middle-aged man with dark hair and glasses, wearing a dark suit, white shirt, and a blue patterned tie. He is looking directly at the camera with a slight smile. The background is slightly blurred, showing what appears to be an outdoor setting with some greenery and a table with bottles.

Role of Police While Dealing with Children in Need of Care and Protection

In India, children constitute almost 40 percent of the population of our country. According to an international legal instrument called United Nation Child Rights Convention – 1989, any one below the age of 18 comes under the children category. All member countries of the UN except the USA have already ratified this legal instrument. India ratified this in 1989.

It's the duty of several stakeholders and uniformed government machineries including the police to protect children.

Child Welfare Officer in all Police Stations

Considering the need for a dedicated police officer to deal with offences and matters concerning children, the JJ Act, 2015 created provision for at least one officer in every police station, not below the rank of an assistant sub-inspector, "With aptitude, appropriate training and orientation" to be designated as the Child Welfare Police Officer (CWPO). The mandate of the CWPO under Section 107(1), JJ Act, 2015 is to "exclusively deal with children either as victims or perpetrators, in coordination with the police, voluntary and non-governmental organizations."

Special Juvenile Police Unit (SJPU)

To coordinate all functions of police related to children, the State Government shall constitute Special Juvenile Police Units in each district and city, headed by a police officer not below the rank of a Deputy Superintendent of Police or above and consisting of all police officers designated under subsection (1) and two social workers having experience of working in the field of child welfare, of whom one shall be a woman.

All police officers of the Special Juvenile Police Units shall be provided special training, especially at induction as child welfare police officers, to enable them to perform their functions more effectively.

The Special Juvenile Police Unit also includes Railway police dealing with children.

Supreme Court's Direction in Sampurna Behura vs Union of India, (2018), 2 SCALE 209

"It is important for the police to appreciate their role as the first responder on issues pertaining to offences allegedly committed by children as well as offences committed against children. There is therefore a need to set up meaningful Special Juvenile Police Units and appoint Child Welfare Police Officers in terms of the JJ Act at the earliest and not only on paper. In this context, it is necessary to clearly identify the duties and responsibilities of such Units and Officers and wherever necessary, guidance from the available expertise, either the National Police Academy or the Bureau of Police Research and Development or NGOs must be taken for the benefit of children."

Facilitation of Care and Protection for Children

According to JJ Act, 2015, the care and protection of children in need of care and protection (CNCP) should be primarily entrusted with the child welfare committee (CWC). Other stakeholders in the system are also entrusted with certain duties towards ensuring that the child receives appropriate care and protection. The police, being one of the key stakeholders coming in contact with children, are mandated to follow certain protocols with

regard to children in need of care and protection.

Child in Need of Care and Protection (CNCP)

According to JJ Act, 2015, the term "child" is defined under Section 2(12), to mean "a person who has not completed eighteen years of age." A police official coming in contact with a child must prima facie ensure that the child is in fact a 'child in need of care and protection' as that will require them to produce such a child before the CWC. It is obvious to take note that the duty to provide care and protection to children is an integral function of the police with other official duties. Some children in need of care and protection are: child labours, children on the street and children of street, children at railway terminals or any other transport terminal, children of red lights areas, including children of prostitutes and child prostitutes, victims of any abuses including sexual abuses, children affected by natural or manmade calamities, in the current context children infected and affected by Covid-19, children affected by substance abuse and so on.

When the victim/offender appears to be a child, treat the person as a child. If there is a doubt as to the victim or offender's age, there is no documentary proof available, or there is a dilemma as to whether the person is a child, take the decision in favour of juvenility and produce the person before the CWC, JJB, or the Special Court, as the case may be, for age determination. Collect documentary proof of age of the victim and the accused promptly. If the child is studying in a school, collect the birth certificate or matriculation certificate from school. If this is unavailable, a birth certificate issued by a Municipal authority or Panchayat should be obtained from the parents. If no

documentary proof is available, inform the CWC or the prosecutor or Special Court so that they can order an ossification test or latest medical age determination test. Do not ask doctors to conduct an ossification test or latest medical age determination test without seeking an order from the CWC/Juvenile Justice

The Special Juvenile Police Unit and Child Welfare Officer at the police station will handle cases of both juveniles in conflict with law and children in need of care of protection and the social worker at the Special Juvenile Police Unit shall be the first line of intervention in all cases, as far as possible.

The Special Juvenile Police Unit shall coordinate and function as a watch-dog for providing legal protection against all kinds of cruelty, abuse and exploitation of children and report instances of non-compliance for further legal action.

The Special Juvenile Police Unit

shall take serious cognizance of adult perpetrators of crimes against children and ensure that they are apprehended immediately and booked under the appropriate provisions of the law.

The Special Juvenile Police Unit shall ensure the registering; linking and monitoring of information regarding missing children received at the police station, and shall investigate immediately.

The Special Juvenile Police Units shall work with voluntary organisations, local governing bodies, community based organisations in identifying juveniles in conflict with law as well as reporting cases of violence against children, child neglect, child abuse and exploitation.

The Special Juvenile Police Unit shall maintain a list of NGOs/voluntary organisations in their respective jurisdiction, and shall monitor the activities to prevent all crimes against children, specifically trafficking, illegal adoption and detention of children.

The Special Juvenile Police Unit to establish & maintain contacts with experts from various fields with the right credentials for their

assistance/cooperation in child related matters, as and when required.

Procedures at Special Juvenile Police Unit

As soon as a juvenile alleged to be in conflict with law is received by the police, the concerned police officer shall inform

- i. The designated Child Juvenile Welfare Officer in the jurisdictional police station to take charge
- ii. The parents or legal guardian of the child or juvenile and their presence shall be ensured during further enquiries, and during any further questioning of the juvenile or child, shall try to ensure the presence of the parent or guardian
- iii. The Probation Officer concerned, to enable him/her to fill in the Social Investigation Report Forms
- a. The juvenile or child shall be treated with decency and dignity during investigation, enquiry, search, etc.
- b. The right to confidentiality and privacy of the juvenile/child shall be upheld.
- c. Police officers and social workers shall ensure that no child/juvenile is tortured or harassed in order to extract information and he or she is not compelled to confess or give testimony.
- d. The Child Welfare Officer or the social worker shall ensure that the juvenile or child is provided with immediate medical attention, basic needs and create a child-friendly atmosphere at the time of first contact.
- e. The Special Juvenile Police Unit shall explain to the child/juvenile the charges against





him/her in a simple language and manner that he/she understands clearly.

A quick assessment shall be made by the Child Welfare Officer at the place of contact and the details shall be recorded in the register/form concerned. The Child/Juvenile Welfare Officer from the jurisdiction police station shall exercise the power of apprehending the child/juvenile only in cases of his alleged involvement in serious offences (entailing a punishment of more than seven years of imprisonment for adults). In cases of non-serious offences where apprehension apparently seems to be in the interest of the child/juvenile, the Child/Juvenile Welfare Officer shall rather treat the juvenile as a child in need of care and protection and bring him/her before the Board, clearly explaining the juvenile's need for care and protection in his/her report and seek appropriate orders from the Board under the rules. For all other cases involving offences of non-serious nature (entailing a punishment of less than 7 years imprisonment for adults) and cases where apprehension is not necessary in the interest of

the juvenile, the Child/Juvenile Welfare Officer shall intimate the parents or guardian of the juvenile about forwarding all information to the Board, which shall have the power to call the juvenile for subsequent hearings. The District Child/Juvenile Welfare Officer at the Special Juvenile Police Unit or the Child Welfare Officer at the Police Station shall ensure immediate registration of a first Information Report in case of juvenile in conflict with law where the offence alleged to have been committed by the juvenile is of a serious nature such as rape, murder or when such offence is alleged to have been committed jointly with adults and age verification done.

After taking charge of the juvenile or child, the Child/Juvenile Welfare Officer shall conduct the preliminary inquiry and arrange to present the child before the Committee in case of a child in need of care and protection or in the case of juvenile in conflict with the law before the Board under intimation to the Special Juvenile Police Unit.

The FIR shall not contain any self incriminating language which can

be held against the child or juvenile.

The police apprehending a juvenile in conflict with law shall in no case place the juvenile in lock-up or delay handing over the juvenile to the Child/Juvenile Welfare Officer. The police shall handle the juveniles or children in civil clothes except while on duty at the time of taking charge of the juvenile. The Child/Juvenile Welfare Officer shall ensure that the police shall not use handcuffs, leading chains or bands while taking the child to the Board, Committee or JJ Homes. In case of a girl child or juvenile, she should be accompanied by a woman police officer.

The Child/Juvenile Welfare Officer shall ensure that no photograph or the identity of the juvenile or child is revealed to the media, no Dossiers/Search Slip etc. shall be opened by the police station and no biometrics/fingerprints of the child is obtained.

The Child/Juvenile Welfare Officer shall ensure that the police do not, under normal circumstances, take charge of a juvenile or child between sunset and sunrise except in unusual circumstances.

Whenever a juvenile is brought before the Board, the police shall furnish the following details: Date and time of taking charge of a juvenile, address of the juvenile, offence said to have been committed and the place where the juvenile was kept stating reasons for delay, if any, till the juvenile was brought before the Board

- Copy of the intimation letter sent to the Probation Officer or parent/guardian of the juvenile
- Details of the property or articles taken from the juvenile at the time of taking charge
- Copy of the First Information Report (FIR), if any.

A juvenile who has committed petty offences may be released after admonition or reconciliation from the Special Juvenile Police Unit or Police Station itself, ratified by at least one member of the Board. If not, the juvenile shall be transferred or retained in the Observation Home/ place of safety/Fit Institution and brought before the Board.

When a juvenile/child is taken into custody for allegedly committing a serious offence, then he/she and his/her parents/guardians shall be informed about their right to representation and an opportunity provided to meet their Legal Aid before the meeting with the Board.

In case the Board is not sitting on the day the child is received, the juvenile shall be brought before a single member of the Board, as per the provisions laid down under the Act, and an order obtained. Such an order shall be ratified by the Board at its next sitting.

The Government shall recognise only such voluntary organizations that are in a position to provide the services of voluntary probation, counselling, case work, a safe place and also associate with the police or the Child Welfare Officer from



the Special Juvenile Police Unit, and have the capacity, facilities and expertise to assist the Police at the time of apprehension, in preparation of the Social Investigation Report, in taking charge of the juvenile until he/she is brought before the Board, and in actual presentation of the juvenile before the Board within twenty-four hours.

The police shall ensure that the provisions of the Convention on the Rights of the Child as well as the Juvenile Justice Principles as enshrined in the J.J Act 2015, are strictly adhered to and all actions are initiated in the best interest of the juvenile or child. We have to remember police forces are the ambassador with regard to restorations of child rights.

I will end this article with a few positive comments about police authority in particular Kolkata Police. I am honoured to be associated with the noble endeavour of the Community Policing wing of Kolkata Police-Nabadisha Programme. A programme that has created a benchmark to uphold the child friendly image of Kolkata Police. This has been implemented since 1999 with the active support from leading NGOs like Vikramshila Education Resource Society, Women Interlink Foundation, Parivar, Maya Foundation etc.

Thousands of school dropouts were brought under education, many of them have completed school as well as their higher studies. This unique programme has saved many children from being trapped into the darkness of the crime world. It establishes positive links between police and community. Because of the programme of this nature, the endeavors of the Kolkata Police was recognised and acknowledged in the UN report called "State of world Children 2003 and Kolkata Police was mentioned as 'Child friendly police force of the City of Joy'.

The Author is a Senior Child Protection Specialist and Psychological counsellor and associated with Vikramshila Education Resource Society as Head - Child Protection, Advocacy and Human Resource.

Acknowledgements and Reference

A handbook on legal processes for the police in respect of crimes against children by - Dr. P. M. Nair and others. •

Satya Gopal Dey
30, Purbachal Lal Bahadur Shastri Road. Postal No - 6, Nandanik Apartment, Flat - 2, Block A, 1st Floor Kolkata - 700078

Rising

Cybercrime Cases

How to Stay Safe From Them



*Hrithik Lall
Chief Technical Officer
IEM Labs*



We came across the word cybercrime several years ago, but now the word gives us shivers. This issue has affected the daily lives of almost every one of us. The way the cybercrime network is constantly expanding, it is beyond the imagination of the common people.

Every day, in every new way, some people are spreading the net of deception and crime. These cheaters are like the rats who, if their way of committing a crime is blocked, they will find a new way to commit it. So we have to be careful and for that, we are giving some detailed information through which everyone can understand how the common man can be saved from cyber fraud.

As per the last five years data from the NCRB (National Crime Records Bureau), in 2016, the cybercrime cases all over India were 12,187, in 2017 it were 21,593, in 2018, it rose to 27,000, while in 2019, the cases increased to 44,395 and then in 2020, it became 49,000 in all over

India.

So, just take a look at the case numbers of 2016, you can see the numbers rose four times by 2020.

Just in a span of 4 years, you can think of which situation the people of India are going through. We have found some selective cases of cybercrimes which are leading in the terms of cases in India. These cases usually occur on a large-scale, simply due to the negligence and lack of knowledge of the common people. If everyone can be made aware of how it is possible to create awareness against it, then it can be checked in many ways. Here, we are going to give a few cases and their details with the possible remedies to stay safe.

West Bengal has also seen a spurt in cybercrimes against women between 2018 and 2022, according to the National Crime Records Bureau

(NCRB).

Cases have increased by five fold in four years and majority of come under the sections of cyber defamation, harassments through e-mail, female child pornography, cyber bullying etc.

According to the NCRB, the number of cases reported in West Bengal in 2018 was 148, which increased to 203 in 2019. It went up to 466 in 2020 and 1,304 cases in 2021. However, it is alarming as NCRB points out that 965 cases have been reported till date in Bengal since the beginning of 2022.

1. Cheating Personation by Using Computer Resource

It's clear from the topic culprits use any computer devices to cheat a person, or an organisation.

This type of cybercrime happens mostly in India, the statistics of NCRB states. What are the possible remedies to stay alert from this type of crime? Some Dos and Don'ts are mentioned below.

Dos

1. Always protect your handset or computer devices with proper security pins.
2. Keep your file protected and software updated to the latest version
3. Always keep the anti-virus and malware function on.
4. Use multiple types of passwords for multiple applications and softwares. Avoid using birth dates, nicknames, lovers name etc.
4. If you see that there has an attack on your devices, instantly inform the police station and tell everything to the authority.

Don'ts

1. Don't tell your passwords to everyone and don't allow anyone to control your device.
2. Don't ignore the security policies of your device.
3. If your device is under an attack, don't hide it from the police.

2. Sexual Exploitation

As far as numbers are concerned, sexual exploitation cases directly comes after the fraud and cheating cases. Sexual exploitation of children has been observed in maximum number of cases in India and the frightening news is that from 2020 the numbers of cases are increasing rapidly. Sexual exploitation means when someone is dependent on any other person for their needs and income and that person seeks sexual favours in return, without consent. In a maximum number of cases, they target children as they are immature and vulnerable.

Children now-a-days are more attracted towards the phone and online gaming world. This gives an opportunity to the exploiters to reach out to children. Unknowingly, they fall into a trap and get exploited. Maharashtra has reported the maximum number of cases of child sexual exploitation while Uttar Pradesh, Assam comes in next. So, what should be done to prevent such cases:

1. Tell them about their body parts. Many children don't know the exact name of their private parts. Please talk to them with the exact name of private parts so that if someone reaches out to children and tries to exploit them, they can tell their parents.
2. Teach them about private parts and if someone asks for those parts, then they should avoid the conversation and report to their parents.
3. Tell them that no one should take pictures of their private parts. If someone does, just report it to parents ASAP.
4. For the parents, if you see your children getting abused or becoming silent day by day, ask them what happened, maybe there might be any reason behind that. Lodge a complaint with your nearby police station and inform the child security cell of your state also.

3. Cyber Blackmailing and Spreading Piracy

Cyber blackmailing & spreading piracy is the most common crime that happens in our surrounding. The current generation, both adults and teenagers, are interested in dating. This thing can make you the victim of this crime. Believing a person and sending him your private photos or videos, can land you in trouble. The viral videos nowadays give them a chance to

defame a girl or a woman.

The videos shot during any private time of yours can be spread on social media by any person you don't even know. A survey states that, 35% of suicide cases of woman nowadays are happening due to this cyber blackmailing and spreading piracy. So there are some tips from us that you could use to save yourself from falling into such traps.

1. Don't believe someone blindly and send your unseen, private photos of good times. Those photos may be the weapon against you in this cyber war.
2. Don't record or keep any private photos in your cellphone that can make you a victim of this crime.
3. Always avoid using fake dating apps and people from any social media account. You don't even know who they are.
4. If you see someone spreading your privacy, don't be afraid, don't get weak. The police and the law have everything to support you
5. Complain to the police, lodge an FIR against suspects, inform the woman safety cell and cybercrime department ASAP.

Apart from these, there are some more types of cyber crime cases like defamation, fake profile creation etc. To save yourself from such cases, please don't indulge into any conversation with someone you don't know because if someone knows your weakness, they can hurt you heavily. So be careful and cautious

Last but not the least, all we can say is that you can get relief if you approach the police and the law without fear. The system always strives to provide protection and justice. All of you stay well, be careful and cautious. •



ATHA GROUP

Head Office: Avani Signature, 6th Floor, 91A/1, Park Street, Kolkata- 700016

Mining | Renewable Energy
Power | Steel | CPC



Right people. Right products. Right services & solutions.

TO HELP OUT CUSTOMERS SUCCEED.

Give Us a Missed Call : 08081112244
Visit Us : www.gainwellindia.com

CAT, CATERPILLAR, their respective logos, "Caterpillar Yellow," the "Power Edge" trade dress as well as corporate and product identity used herein, are trademarks of Caterpillar and may not be used without permission. © 2018 Caterpillar All Rights Reserved.





TEJASWINI

In a step towards women empowerment, the Kolkata Police announced the five-day self-defence course 'Tejaswini' exclusively for women in 2018. The first edition of Tejaswini was organized by the Kolkata Police from May 19-23, 2018. It was immensely successful and witnessed the participation of over 350 women aged between 26 and 30 from different schools, colleges and other fields.

The motto of Tejaswini is to teach women basic self-defence techniques to enable them to counter unwanted physical advances including molestation, sexual harassment in buses, trains, simply walking along the road, in workplaces, or even in their own homes. The biggest advantage of Tejaswini is that one doesn't need to have any previous experience to learn these self-defence techniques. Anyone can participate in this landmark initiative by Kolkata Police. In the Covid phase, Tejaswini was held in the virtual mode. Last year, the Tejaswini workshop also included training on cyber crime and legal expertise to the participants.

-

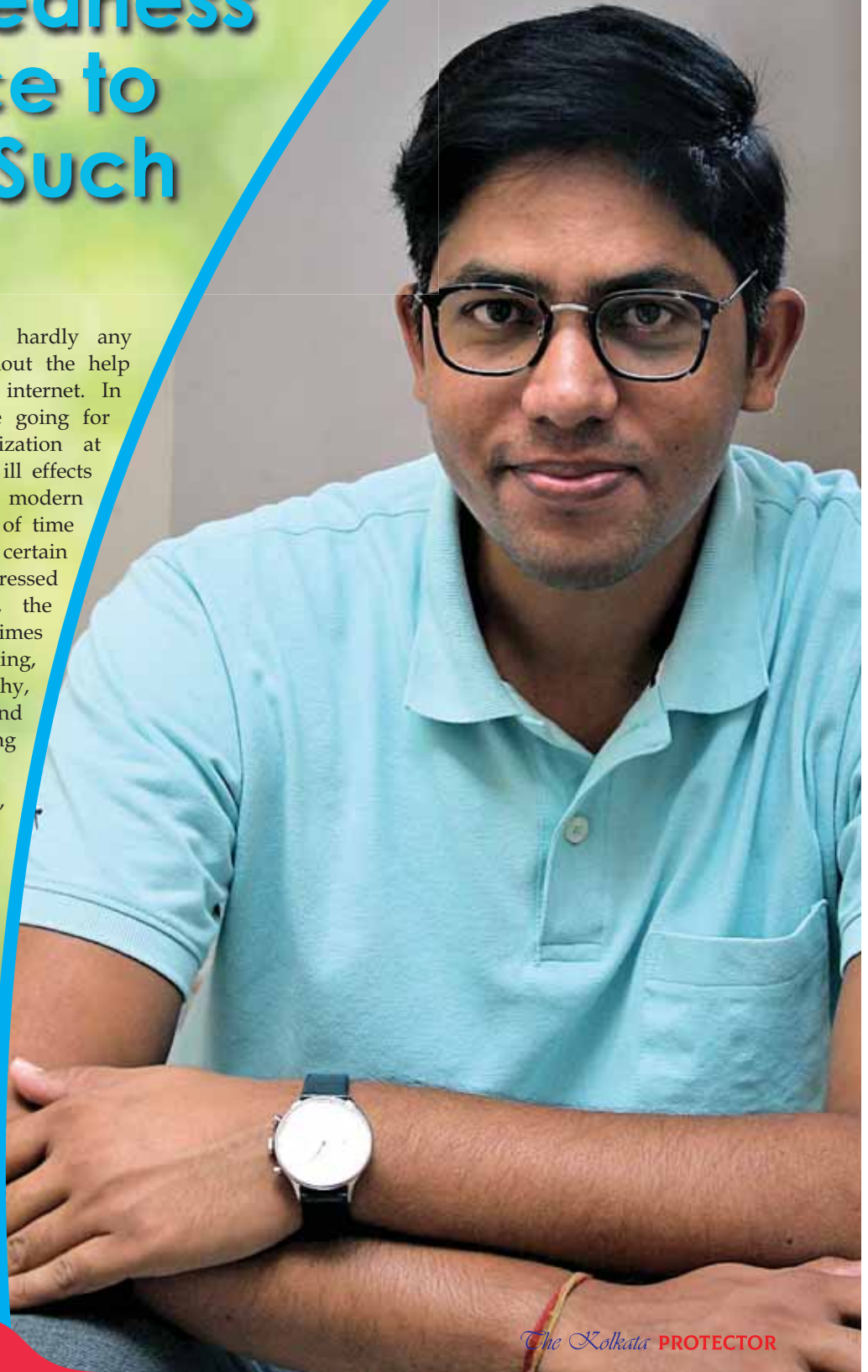




Changing Face of Cybercrime and Preparedness of Police to Crack Such Cases

In this dazzling world, hardly any work can be done without the help of technology and the internet. In the present era, people are going for modernization and digitalization at such a fast pace so that its ill effects are drastically being felt in modern society. But for some point of time we can ignore its ill effects, as certain serious issues need to be addressed immediately. For example, the investigation and control of crimes such as cyber fraud, stalking, harassment, pornography, sexting, espionage and ransomware are the pressing concerns.

According to the NCRB report, cyber-crime has registered a growth of around 12% in the year 2020. During 2020, 60.2% of the total cybercrime cases registered were for fraud (30,142 out of 50,035 cases), followed by sexual abuse with 6.6% (3,293 cases) and extortion with 4.9% (2,440 cases). These figures are probably incomplete, as only one third of cybercrime cases are registered in India and many complaints never get converted into



FIRs. The reality is that cybercrime is increasing at a rate of about 200% every year and new threats are emerging. The police and the law machinery will have to make extensive preparations to control the rising cybercrime cases.

Upcoming Cyber Threats

Today, mainly cases related to financial frauds, and digital account hackings are coming to the fore. In the future, many new and serious cyber threats are going to come out. This would not only be new in methodology, but would also require a state-of-the-art cyber lab along with a skilled team to deal with it.

Data theft, hijacking and alteration would be the huge threats to every government and non-government organizations. For example, in digitisation today almost every hospital has started to put the diagnosis and consultation data of patients online. And in many high-tech hospitals, the treatment is also fully automated, where the machinery determines the oxygen level for the patient and the amount of medicine in the glucose bottle. If the hacker is able to hack the automation and smart hospital system, it can cause the hospital system to malfunction and even cause loss of life. Similarly, hacking of Internet of Things (IOT) and smart vehicles can also have dire consequences.

Guidelines

To prevent cyber crimes, the Government of India regularly issues guidelines for many social media and online service providers. In February, 2020, the Indian government had issued an official guideline for social media intermediaries and OTT platforms. India's former IT, Law and Justice Minister Ravi Shankar Prasad had said that "Social media companies should accept requests to remove

illegal, misleading and violent content within 24 hours and provide full redress within 15 days".

On 28 April, 2022, the Indian Computer Emergency Response Team (CERT-In) issued new directions under Section 70B (6) of the Information Technology Act, 2000 (IT Act), that it is mandatory for service providers, intermediaries, data centres, companies and government organizations to report cyber incidents within six hours.

Preparedness of Police

Nowadays, criminals are using high-end computer devices and virtual platforms. They are quite capable of hiding their identity with the help of virtual private network (VPN), virtual number, temporary email ID and rented bank accounts. Therefore, the investigating approach and methodology of the police should fasten their belts to be able to crackdown on cyber incidents of the next level. Every police station should have a strong capability to investigate cyber-crime cases effectively.

The cyber forensic laboratory should have sufficient capacity and bandwidth to examine all digital devices, cloud and online accounts in a short time. Today, it takes many months to get the evidence test report from digital forensic labs because the number of labs are few, and on top of that many labs do not have enough equipment, and many do not have skilled manpower. To effectively handle new cyber-crime cases, police personnel should be given case study oriented training regularly. Several crucial changes need to be implemented in the police recruitment process, such as a special drive to recruit cyber experts.

Preparedness of Judiciary

The Indian judicial system, which has been running for the last 73 years, probably does not have the

power to take tough decisions in cases related to cybercrime. There can be two possible reasons for this, firstly the vastness of the cases pending in the court and secondly the lawyers and judges do not have enough knowledge of the cyber world. There is a dire need to enact a strict law to make the judiciary more strong and effective. Along with the new law, there is also a need to amend the IT Act 2000 so that all avenues of escape for criminals are closed and almost every offence should be made non-bailable.

Dedicated courts and trained judges should be arranged for cyber-crime cases. Lawyers and judges should be trained regularly to make the judicial system more reliable and effective. There should be strict provision of punishment and fine in the law so that no one dares to commit such an offence. •

Author:

Ummed Meel

Designation: Cyber Expert (Police and Defence Advisor)

Education: B Tech, LLB (Cyber Law), CISA, CEH, CHFI, DCL

Ummed Meel is a renowned cyber expert (Police and Defence Advisor). He has been invited as an expert in more than 100 training and workshops on cybersecurity, intelligence, and cybercrime investigation for Ministries including State Police, India Air Force, BSF, CISF, CAG, BPRD, CDTI and other law enforcement agencies. He has 7+ years of experience in cybersecurity, VAPT, Digital Forensics and Cybercrime Investigation. His articles have been published in many world renowned magazines. He has also been interviewed by several news channels and newspapers for expert views on cybercrime. In addition, he has delivered over a hundred lectures in seminars on cyber-crime awareness in schools, colleges and universities. He has also assisted various investigative agencies in solving around 200 major cases related to cyber-crime in the country.



Destroy your Data Before it Destroys you!

Nandan Mall
Founder & CMD,
Hulladek Recycling Pvt Ltd.

There are many concerns associated with the modern cybersecurity community. Robust firewalls, reliable cloud storage solutions, in-house IT support and antivirus bundles are all examples. Still, the role of data destruction should never be taken for granted.

Most of us are already familiar with data destruction from a basic point of view. Common examples include rather traditional processes such as shredding or incinerating documents when they are no longer needed. However, it is just as important to remember that we live in a digital age. To put it another

way, such methods often prove to be outdated.

Data destruction now involves the complete annihilation of information, specifically, when contained within a digital storage device. The role of physical concerns should be examined as units such as hard drives, smartphones and outdated laptop computers need to be disposed of properly to avoid posing security risk.

Hulladek Recycling is an e-waste management company that collects and channelises electronic and electrical waste. Licensed and authorised by the Central Pollution Control Board, they have successfully recycled 2 million kgs of e-waste. Headquartered in

Kolkata with a presence in 18 states across the subcontinent, they are working with some of the corporate giants such as PepsiCo, Nestle India, Mondelez International, Berger Paints, Tata Steel and many more. Apart from collection of waste from bulk consumers, they also provide door-to-door service to households, reaching about 500 unique households every month. When dealing with such vast quantities of waste, it is imperative that they assure security and safety of their clients.

One of the challenges associated with the cybersecurity industry is that digital data can leave a much larger footprint when compared to physical documents. In the past,

shredding sensitive materials could very well have been all that was required to ensure that information did not fall into the wrong hands. That is hardly the case with digital data. This is also why more innovative techniques have been developed. There are 3 common ways to dispose of digital information:

- Overwriting a storage device
- Degaussing
- Physical destruction

As the term already suggests, overwriting data involves placing an additional layer of information atop existing material. The main purpose is to ensure that the hard drive itself is not damaged while still covering up the information that it contains. However, it should be noted that this technique can sometimes be rendered ineffective by someone who possesses a significant amount of technical experience.

Degaussing is another option. In this case, a strong electromagnet is passed over the storage device. These magnetic fields will essentially scramble all the information that is present, rendering it completely unreadable. The only possible concern here is that such a technique also damages the device itself. Degaussing is still one of the most common and cost-effective ways to ablate information.

Finally, it is always possible to physically destroy the device in question. This can be performed using chemicals or by shredding the unit. The only potential problem is that even a hard drive or device that has been physically destroyed may still contain an appreciable amount of data. Therefore, many organizations choose to outsource such solutions to qualified third parties.

Electronics are known to be a storehouse of data, which can easily be hacked or leaked. Data destruction is the best way to ensure that data does not fall into the wrong hands, which could cause untold damage to an enterprise's finances and reputation. This is particularly important when decommissioning equipment, especially if it is going to be resold or recycled. While handling a capacity of 2,000 tonnes annually, maintaining data security and privacy is of utmost importance.

Hulladek deals with a diverse range of industries including financial institutions and government departments, where data security is a primary concern. Our customers remain confident that sensitive information will not fall into the wrong hands. Customers are also becoming extremely particular in terms of the organizations with which they choose to work. As the risk of insufficient cybersecurity becomes more familiar (even to those with little technical experience), it only

stands to reason those enterprises offering modern solutions will be preferred. To put it simply, adopting the correct approaches is good for business.

The first factor to consider is the type of hardware that is being used to store data. Creating audits and logs is the best way to determine when a specific device should be destroyed. Time is another major issue, as organizations need to ensure that these processes will not impact their ongoing operations. Lastly, what is the reputation of the data destruction enterprise in question? Have previous customers left positive or negative opinions of their experiences? How long has it been in operation and does it comply with all relevant statutes? What types of client support solutions are offered? Fortunately, there are many organizations like Hulladek Recycling that have considerable experience within this dynamic field.

In today's digital age, cybersecurity is a trending topic for organizations that are under constant threat from cybercriminals. However, it is essential for business owners to understand that data no longer in use is still a target of fraudsters. For this reason, an effective data destruction policy is essential to avoid costly data breaches.

[illegible]

Winners TEAM

The all-women 'Winners' team of Kolkata Police was initially raised on July 11, 2018. The focus was primarily to prevent crime against women in areas under the jurisdiction of Kolkata Police, inspired by West Bengal Chief Minister Mamata Banerjee, who herself gave the name to the all women patrolling team.

The first team had a total of 27 personnel, including two Sub-Inspectors, one Assistant Sub-Inspector and 24 Constables. The team was inducted into the Kolkata Police following a month's training. The duties include patrolling areas such as parks, shopping malls, educational institutions, and other vital locations, including night patrols. The Winners team has done a commendable job during festivals like Durga Puja, Christmas, New Year's Eve, Eid etc. Seeing the success of the team, the Chief Minister has instructed to make Winners Team in all Municipal towns and Police Commissionerates.







Utsarga

Utsarga, the voluntary blood donation initiative of Kolkata Police, has received tremendous response over the years. Throughout the year, the community policing wing of the Kolkata Police has been integral to organising blood donation camps at various places under the jurisdiction of Kolkata Police. Utsarga has been a noble endeavour on behalf of the Kolkata Police in meeting the increasing demand for blood.





Brain Tumours and their Treatment Procedures

Prof (Dr) R.N. Bhattacharya,
MS, M.Ch Director,
Neurosciences AMRI Hospitals, Dhakuria

The brain is the command centre of our entire system; it controls all our activities and the entire body. When a tumour grows or cancerous cells develop in the brain, it affects our entire system and the body finds it difficult to function. **Prof (Dr) Bhattacharya** explains about brain tumours, available treatments, and chances of cure.



How many types of tumours are there?

Tumours are of two kinds -- benign, and malignant. A benign tumour is usually slow-growing and may not show any symptoms until the tumour puts pressure on the brain and prevents a specific area from functioning properly. Malignant tumours are deadly and fast-developing, with the symptoms varying according to the type and location. While primary tumours develop in the brain, secondary tumours are cancerous cells that spread to the brain from organs like the lungs, kidney, breast, or skin.

What are the symptoms of brain tumour?

The primary symptom of a brain tumour is a severe headache so that it feels like the head will explode.

to just one side of the head, there is less chance that a tumour is present. Severe nausea, mostly in the morning, along with hazy vision, particularly the far sight, are also noticeable symptoms.

What is the treatment procedure for a patient suffering from tumour and how is it decided?

Treatment for brain tumour depends on factors like shape and size, location, extent, and grade, or level of its fatality. A person's age and overall physical condition is also important. The patient has to undergo tests like MRI, CT scan and PET scan for better understanding of these factors, and a biopsy is done to determine if it is

like micro surgery, endoscopic surgery, and image-guided surgery lessen damage to brain tissues and can help remove tumours almost totally. For malignant tumours, radiotherapy and chemotherapy are used post-surgery.

What type of life can a patient lead after surgery?

Patients suffering from Stages I and II of malignant tumour can live a controlled and supervised life after surgery. Those in Stage III usually do not live beyond five years, and it is impossible to cure those in Stage IV, with their average survival period being not more than 18 months. Although it is not always possible to extend the duration of a person's life, quality of life can definitely be improved. ●

List of Senior officers of Kolkata Police

Officials Name	Name	Phone
Commissioner of Police	Shri Vineet Kumar Goyal IPS	2214-5060
Spl Commissioner of Police (I)		
Spl Commissioner of Police (II)	Smt. Damayanti Sen IPS	2214-1696
Addl Commissioner of Police (I)	Shri Hari Kishore Kusumakar IPS	2214-5950
Addl Commissioner of Police (II)	Shri Laxmi Narayan Meena IPS	2214-1767
Addl Commissioner of Police (III)	Shri Debasish Boral IPS	2214-1055
Addl Commissioner of Police (SB)	Shri Rajesh Kumar Yadav IPS	2282-3602
Addl Commissioner of Police(IV)		2214-5476
Jt. Commissioner of Police (HQ)	Shri Subhankar Sinha Sarkar IPS	2250-5207
Jt. Commissioner of Police (TP)	Shri Pandey Santosh IPS	2214-5558
Jt Commissioner of Police (PRB)		2283-7671
Jt Commissioner of Police (Intel)	Shri C. Sudhakar IPS	2282-5957
Jt Commissioner of Police (O)	Shri Syed Waquar Raza IPS	2214-5509
Jt. Commissioner of Police (A)	Shri Ashesh Biswas IPS	2214-1836
Jt Commissioner of Police (AP)	Shri Nilanjan Biswas, IPS	2479-3554
Jt. Commissioner of Police (Crime)	Shri Murli Dhar IPS	2214-5737
Jt. Commissioner of Police (STF)	Shri V. Solomon Nesakumar, IPS	2214-1354
Jt Commissioner of Police (Establishment)	Shri Akhilesh Kumar Chaturvedi, IPS	2214-0030
Jt. Commissioner of Police,SB (Security)	Shri C. Sudhakar IPS(Addl. Charge)	2282-0631
Jt Commissioner of Police (Training)	Shri Mehmood Akhtar IPS	2657-4050
Deputy Commissioner of Police, Cyber Crime	Shri Praween Prakash, IPS	2250-5010
Deputy Commissioner of Police, STF	Shri Harikrishna Pai IPS	2264-0023
Deputy Commissioner of Police (Special), Detective Department	Shri Surya Pratap Yadav , IPS	22505222
Deputy Commissioner of Police(II), Special Branch	Shri Tarak Pyne	2282-2090
Deputy Commissioner of Police(III), Special Branch	Smt. Mousumi Paul	2282-0031

Deputy Commissioner of Police, Wireless Branch	Col. Nevendera Singh Paul	2283-7656
Deputy Commissioner of Police, Enforcement Branch	Smt. Bidisha Kalita IPS	2283-7700/7560
Deputy Commissioner of Police, Reserve Force	Shri Subhankar Bhattacharya, IPS	2214-3366
Deputy Commissioner of Police(II), Security Control Organisation	Shri Goutam Nanda	2287-5881
Deputy Commissioner of Police, Traffic Department	Shri S. K. Yadav, IPS	2214-5403
Deputy Commissioner of Police (South), Traffic Department	Shri Atul V, IPS	2499-4703
Deputy Commissioner of Police (II), Traffic Department	Shri Maksud Rahaman Sardar	2214-5803
Deputy Commissioner of Police (III), Traffic Department	Shri Anuj Home Roy	2214-1830
Deputy Commissioner of Police, HGO	Shri Tapan Saha	2409-9371
Deputy Commissioner of Police, 1st Bn, KAP	Shri Arish Bilal, IPS	2409-9054
Deputy Commissioner of Police, 2nd Bn, KAP		2557-5050
Deputy Commissioner of Police, 3rd Bn, KAP	Shri Arindam Sarkar, IPS	2409-9096
Deputy Commissioner of Police, 4th Bn, KAP	Shri Saikat Ghosh, IPS	2337-3320
Deputy Commissioner of Police, 5th Bn, KAP	Smt. Sujata Kumari Veenapani, IPS	2355-9007
Deputy Commissioner of Police, 6th Bn, KAP	Shri Ujjal Hazra	2409-9055
Deputy Commissioner of Police, 7th Bn, KAP	Shri Subrata Kumar Paul	2409-9056
Deputy Commissioner of Police, 8th Bn, KAP	Shri S. Raju	2530-0817
Deputy Commissioner of Police, Combat Battalion	Shri Sukhendu Hira IPS	2262-5222
Deputy Commissioner of Police, IUCAW, DD	Smt. Mangola Biswas	2214-1953
Deputy Commissioner of Police, Women Police	Smt. Mousumi Paul	2953-0100
Administrative Officer, KPD	Shri Hardeep Singh Jagpal, WBCS (Exe.)	2214-3059



You are your city's eyes & armour

INFORM POLICE ABOUT



Unidentified Objects



Abandoned Vehicles



Suspicious Persons



Dial-100 /1090

KOLKATA POLICE
ALWAYS WITH YOU

BEYOND
55
YEARS
OF GLORIOUS JOURNEY
1967 - 2022

**KOLKATA'S
MOST TRUSTED
PREMIER
HEALTH CARE
INSTITUTION**

**24hr
SERVICE
EVERYDAY**



CT SCAN, MRI, PATHOLOGY, X RAY, PHARMACY, DIALYSIS, BLOOD BANK, AMBULANCE, EMERGENCY, AMBULANCE, DIALYSIS

9 & 10 Dr. U.N. Brahmachari Street (formerly Loudon Street) Kolkata- 700017 Ph: 033 6688 8888

**THE CARE OF
HEALTH CARE
IS NURSING**



PRIYAMVADA BIRLA INSTITUTE OF NURSING
(Unit of Belle Vue Clinic)

Priyamvada Birla Institute of Nursing by Belle Vue Clinic strives for excellence and aims at providing value based nursing education, moulding students into skilled and efficient nurses who can serve competently both in India and abroad.

**Strictly follows the regulations of the
Indian Nursing Council**

**Students gain complete experience in various specialities
with latest diagnostic equipment**

Affiliated under Indian Nursing Council (INC), West Bengal University of
Health Sciences (WBUHS) and West Bengal Nursing Council (WBNC)

Located at Newtown, Rajarhat

Courses offered:
**GNM Nursing, B.Sc.
Nursing, Post Basic B.Sc.
Nursing, M.Sc. Nursing**

For more information on admission: Phone : 7608065329/7516067192/94/95

IIF/9, AA- IIF, Newtown, Rajarhat, Kolkata - 700 156 Beside the Eco Space