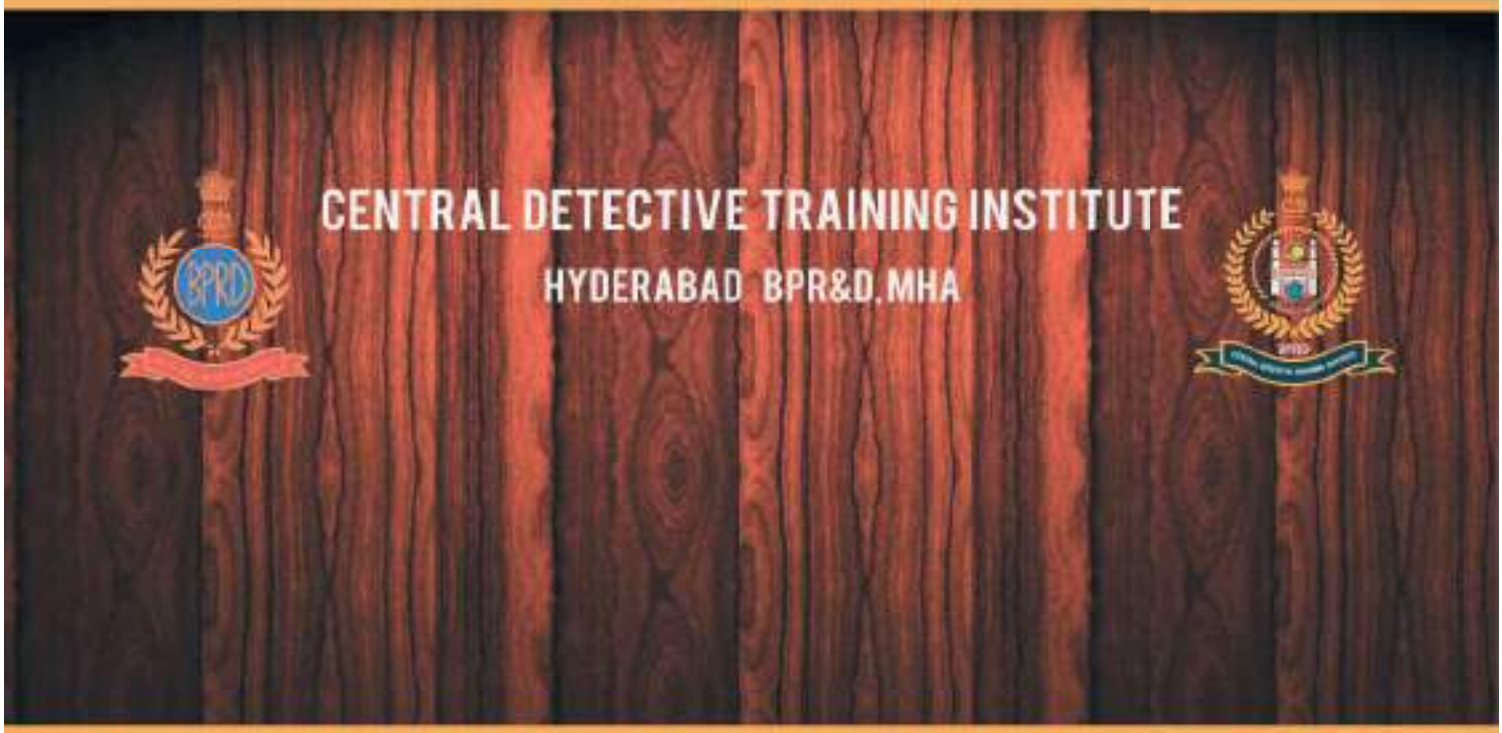
July - Sept 2024

CDTI, HYDERABAD

Bulletin

HORIZON

Our Motto "*ज्ञानं सम्यग् वैक्षणम्*" which means
"WISDOM LIES IN PROPER PERSPECTIVE"



A Quarterly Bulletin of Central Detective Training Institute, Hyderabad

MESSAGE OF THE DIRECTOR

Shri. Rajashekara N, IPS
Director, CDTI, Hyderabad

It gives me immense pleasure that the Central Detective Training Institute, Hyderabad is going to launch its quarterly year news magazine "HORIZON" for the period July to September, 2024.

CDTI, Hyderabad is declared as Centre of Excellence for "Police Technology, IT and Cybercrime" and coupled with the establishment of "National Cyber Research, Innovation and Capacity Building Centre (NCRI&CB)" under the Indian Cyber Crime Coordination Centre (I4C), MHA, enabled CDTI-Hyderabad to hone the investigative skills of police officers in the field of cybercrimes. So far 28 courses conducted in this Lab and trained 765 officers. The visit was a great moral booster and privilege for us. CDTI, Hyderabad is most sought after Advanced cyber crime investigation courses.

Apart from CDTI – Hyderabad, we are conducting courses at CDTI, Bengaluru also. We have conducted 05 courses in this quarter at Karnataka Veterinary Council, Hebbal, Bengaluru in the name of CDTI, Bengaluru and trained 188 officers. It also includes three back-to-back courses in the month of Sept, 2024 and the list is as under:

S.NO.	SUBJECT OF THE COURSE	FROM - TO	NO OF PARTICIPANTS
1	Social Media Investigation & Data Analytics	22.07.2024 to 24.07.2024	34
2	Investigation of Crime against Women and Children (POCSO Act)	26.08.2024 to 28.08.2024	45
3	ToT Course on New Criminal Laws 2023	19.09.2024 to 21.09.2024	33
4	SMART Policing	23.09.2024 to 25.09.2024	40
5	Protection of Data and Digital Public Goods	27.09.2024 to 28.09.2024	36

Shri. Rajeev Kumar Sharma, IPS, DG, BPR&D visited CDTI, Hyderabad on 20-09-2024 along with Shri Hemant Priyadarshy, IPS, DGP (Cybercrime), Rajasthan. They interacted with students of St. Joseph's High School, Ramanthapur, Hyderabad for whom an Awareness Programme was arranged.

CONTENTS

ABOUT TRAINING

Central Detective Training Institute, Hyderabad imparts training to the client state police officers of Andhra Pradesh, Telangana, Karnataka, Tamil Nadu, Kerala, Maharashtra, Puducherry, Delhi, Gujarat and Lakshadweep. It also imparts training to Police Officers of other States/ UTs and CRPF, BSF, CISF, SSB, RPF on the courses related to cyber crime cases.Armed Personnel from Army, Navy and Air Forceare also given training on their request.

This year (2024-25), CDTI, Hyderabad got approval from the BPR&D Hqrs for conducting 75 courses which includes Workshops, Webinars, Conferences, ITEC courses and Awareness Programmes. Based on the duration of course, some of the courses of duration one day are conducting in 'Online' and remaining courses in 'Offline' mode.

The institute conducts courses of 01 day, 02 days, 03 days, 5 days and 10 days duration on various topics of contemporary interest concerning modern day policing, besides various Webinars & Workshops', and Awareness Programmes.

COURSES CONDUCTED FROM JULY TO SEPTEMBER, 2024

From 01st July to 30th September, 2024 a total of 19 Courses (including Workshops, Webinars, Conferences) were conducted in which 2884 Officers were trained.

S. NO	NAME OF THE COURSE	DATE		No. of Participants
		From	To	
1	AI, Crypto Currency & Block Chain Technology	01.07.2024	05.07.2024	19
2	Sensitization of New Criminal Laws – 2023	08.07.2024	12.07.2024	206
3	Sensitization of New Criminal Laws – 2023	13.07.2024	14.07.2024	59
4	Workshop on OSINT	16.07.2024	16.07.2024	65
5	Webinar on Investigation of block chain & crypto currency	19.07.2024	19.07.2024	46
6	OSINT (for IAF only)	22.07.2024	26.07.2024	30
7	Windows & Linux OS - for Cyber Crime Investigation & Analysis	22.07.2024	26.07.2024	19
8	Webinar on NCL	27.07.2024	28.07.2024	1903
9	Drones Investigation	29.07.2024	02.08.2024	32
10	Sensitization of NCL (Prison/ Prosecutors)	29.07.2024	31.07.2024	39
11	Sensitization of NCL	05.08.2024	09.08.2024	124
12	Conference on Kali Linux	12.08.2024	12.08.2024	40
13	Handling CCTV footages & DVR forensics	19.08.2024	23.08.2024	35
14	Introduction & Investigation of AI, Crypto currency, Block Chain Technology and Darkweb Transactions	26.08.2024	30.08.2024	27
15	Introduction & Investigation of AI, Crypto currency, Block Chain Technology and Darkweb Transactions	02.09.2024	06.09.2024	32
16	ToT Course on NCL 2023	09.09.2024	11.09.2024	52
17	Workshop on deep and darkweb and block chain forensics	18.09.2024	18.09.2024	50
18	Sensitization of NCL	23.09.2024	27.09.2024	84
19	Webinar on Ethical and Legal implications of AI in cyber crime investigation	30.09.2024	30.09.2024	22
TOTAL				**2884**

CENTRAL DETECTIVE TRAINING INSTITUTE, HYDERABAD

Course on " AI Cripto Currency & Block Chain Technology

01-07-2024 to 05-07-2024

Sitting (L to R) S/Sri :- Sandeep Mudalkar, Cyber Crime Investigator, Dr.S.Karthikeyan, Vice Principal, CDTI, Atharva Singh, AC, CRPF, Rajashekara.R IPS Director, CDTI, Elias - P.George, Inspr(Ker), Mrs.Anusuya Baral, Dy.SP, CDTI, G.Rajkumar Dy.SP, Course co Ordinator, CDTI

Standing 1 (L to R) S/Sri :- Mohit Kumar, SI(Del), Ujjal Datta, ASI(WB), Hari Shubham, SI, CRPF, Manish Suhag, SI(Del), Mrs.Anju, SI(Del), Deepak Banswari, SI(Assam), B.Praveen Kumar -Singh, RSI(AP), Antony, V.J, SI(Ker), Mohammed Wasim Akram, SI(WB), Shiju A.R, SI(Ker).

Standing 2 (L to R) S/Sri :- Anil Kumar Rai, SI(Meghalaya), Biswajit Gadanayak, SI(Odisha), Samar Kumar Das, SI(WB), Sanjit Kumar Mahato, ASI(WB), Kunal Jha, SI(WB), Arun Kumar, SI(Del), Alok Sarkar, Sgt(WB).

CENTRAL DETECTIVE TRAINING INSTITUTE, HYDERABAD

Course on " Sensitization of New Criminal Laws-2023

08-07-2024 to 12-07-2024

Sitting (L to R) S/Sri :- Upasala Venu, Inspr(Addmn)CDTI, Smt.K.R.Valsam, Asst.Public Prosecutor(TN), Dr.K.Sambamoorthy, Advocate, Rajashekara.R IPS Director, CDTI, Dr.S.Karthikeyan, Vice Principal, CDTI, Veeresh G.Mamani, Public Prosecutor(Kar), BM.Bistagond, Public Prosecutor(Kar).

Standing 1 (L to R) S/Sri :- K.Shailashavali, ASI(AP), Mrs.Thejavathi UC, Asstt.Jailor(Kar), M.Sarvamangala, Public Prosecutor(Kar), Mrs.Anupama SK, Public Prosecutor(Kar), Mrs.Asmita Arjun Gawas, LASI(Goa), Mrs.Gurusiddavva Patil, Public Prosecutor(Kar), Mrs.Bandi Swapna, Scientific Officer(TG), Mrs.K.B.Bindu, - Jailor(Kar), Smt. Kavitha HD, Asst.Public Prosecutor(Kar), Mrs.Dr.Vedkonda Naga Laxmi, Scientific Officer(TG), Mrs.Lalita Laxmikant Amonkar, - LASI(Goa), Allimuddin, Asstt.Jailor(Kar).

Standing 2 (L to R) S/Sri :- Mopanthi Kishore Kumar, Deputy Jailor(AP), Rajiv Kumar Turi, Sub-Inspr(Jharkhand), Ramu Ashwapuram, Scientific Officer(TG), Pabdul Razak, ASI(Goa), Surajit Sarkar, Sub-Inspr(Tripura), K.Ravi Kumar Goud, Asstt.Director(TG), Mekunda Shankarao Deshpande, Sr.Asstt.Public Prosecutor(Kar), Raja - Public Prosecutor(Kar), Rahul Saha, Asstt.Public Prosecutor(Kar), Mr.Manjunath Kalyani, Asstt.Public Prosecutor(Kar), Biswas Saha, Sub-Inspr(Tripura), Ratheesh KC, Inspr(Ker).

Standing 3 (L to R) S/Sri :- B.Nagaraju, CA, CDTI, Sanjivo Pandurang Naik Dessai, ASI(Goa), Palati Joseph Sugunkar, Deputy Jailor(AP), Danyasi Srihari, Sub-Inspr(Tripura), Vishwas Babaji Mahale, ASI(Goa), Mahadev Vasanthanoolkar, ASI(Goa), Anant Mahadev Gaonkar, ASI(Goa), Manoj Pandhari Gohekar, ASI(Goa), Siddappagouda N.Patil, Jailor(Kar), Mr.Madduluri Rathaiah, Inspr(AP), M.Manohar Chary, CA, CDTI.

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on " Sensitization Of New Criminal Laws-2023"

29-07-2024 to 31-07-2024

Sitting (L to R) S/Shri :- Nagaraju C,Nalwa,Dr.PP(Ker),Beno Nishant Rubert,Supdt,Principal,Dte/Tumkur,K.Lakshmi Nath , Addl.PP Gr-I(AP),Harikrishna Bhupati Sawant - Judge,Ms.Anusuya Basel, Dy.SP,CDTI,Dr.G.Saijaxi, Addl.PP Gr-I(AP),G.Rajkumar, Dy.SP, Course coordinator,CDTI,Hyd.,Sanjay Durgadi Rao - Deshmukh, Addl.PP(Mah), Mrs.C.S.Sailaja, Addl.PP Gr-II(AP).

Standing ((L to R) S/Sri :- Mrs.K.E.Swarnalatha Reddy,Addl.PP Gr-II(AP), Sk.Mubeena Begum, Addl.PP Gr-I/Spl.PP(AP), Bhumgaiya Mole Ramesh, Addl.PP(Mah), Mrs.Anjaneya Ameya Pandalai, APP(Mah), Ms.Leena Chandrakant Chavan, Addl.PP(Mah), Mrs.D.Sreevani, Spl. Addl.PP Gr-I/Spl.PP(AP), Mrs.PVN Jyotsna Rani, Addl.PP - Gr-I/Spl.PP(AP), Mrs.C.A.Sheretha Law Officer(Jr)(Ker.), Mrs.G.L.Ranganeema,Addl.PP Gr-II(AP), Mrs.B.S.Mamatha,PP(Ker), Mrs.V.Krishnaveni, - Addl.PP Gr-II(AP), Mrs.Namrada.S, APP(Kar).

Standing 2 (L to R) S/Sri :- Md.Bakar Ali Khan,Addl.PP Gr-II(AP), K.Rama Naik, Addl.PP Gr-II(AP), Pukhrat Kumar Supdt(Rajshahi), Niranjan, ASI(Tuticorin), M.Gaikwad, - ASI(Pune Rural), Aziz Masid Shah, APP(Mah), H.S.Lohitaswatha, PP(Ker), B.R.Sathisha,S.I.APP(Kar),Pyla Krishna Nayaka, PP(Kar), B.S.Manjunatha, - PP(Kar), Dwarkanath B.Gite, APP(Mah), N.P.Devendra, PP(Kar).

Standing 3 (L to R) S/Sri :- K.Chenna Krishna, Addl.PP Gr-II(AP), K.Radha Krishna Raju, Addl.PP(AP), G.Vijaykumar Babu, Addl.PP Gr-II(AP), Prashanth Yalagar, APP(Kar), C.Sreenivasulu, Addl.PP Gr-I(AP), L.Balaji, Addl.PP Gr-II(AP), Shanti Bidhi, Asst.Jailor(Kar), Venkatesh, Jailor(Kar), Shashikumar.M, Asst.Jailor(Kar), S.S.Nagaraju, Asst.Jailor(Kar).

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on " Windows & Linux OS-For Cyber Crime Investigation & Analysis"

22-07-2024 to 26-07-2024

Sitting (L to R) S/Sri :- G.Rajkumar,Dy.SP, Course Coordinator,CDTI, Ms.Talyaba Khatoon, TO, NTRO, Sunil Kumar Sharma, TO, NTRO, Mrs.Anusuya Basel, Dy.SP,CDTI, Hiroto I.Zhimomi, ACP, Nagaland, Lakhan Ashok Rao Handebag, Cyber Investigator,Hyd, Uppada Venu, Insp(Admn).

Standing 1 (L to R) S/Sri :- Rajib Mandal, SI(IP), Ravindra Singh, SI/GD, CRPF, Neshale Keluase, Insp(Nagaland), Basidi Kumare Swamy, TO, NTRO, Hemangshu Sarkar, SI(Assam), Anil Kumar, SI(J&K), Budra Rh Suren, SI(Assam), Subhrajyoti Satapathy, ASI(Odisha), Sajeev Kumar Ranjan, SI(Jharkhand), Ajit Kumar, SI(Jharkhand), Narender Singh, SI/GD, CRPF.

Standing 2 (L to R) S/Sri :- Tasleem Chhatterjee, Sgt,IRP WB, Manjur Alam Molla, SI/RP WB, Asaduzaman, ASI/RP WB, Pijush Kanti Mandal, ASI/IP WB, Shyam Sundar Pal, - SI/RP WB.

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on " Drones Investigation"

29-07-2024 to 02-08-2024

Sitting (L to R) S/Sri :- J.Srinivas, Chief Sales Officer,Bangalore), Sudarsan Hombali, Dy.SP(Admn), Abhishek Kumar Gaurav, AC, SSB, Ms.Anusuya Basel, Dy.SP,CDTI, Mrs.SR.Harshitha, DSP(AP), Lakhan Ashok Rao Handebag, Cyber Investigator,Hyd, Uppada Venu, Insp(Admn).

Standing 1 (L to R) S/Sri :- S.Praveen Kumar, SO(AP), Anku Saikia,Si(Assam), Kinnar Sahu,Si/Tripura,Santhosh Chandra Reddy, Si(WB),Vinod, Insp, SSB, Mrs.Tanveen Akhter, TA, NTRO, Ratur RL, Si/Che(Pon), Vidyadhar Das, Si(Assam), Anurag K, Si/Che(Pon), Mohammad Sohni, SI/OD, CRPF, Ram Shankar Prasad, Insp, SSB,

Standing 2 (L to R) S/Sri :- Sruthi S, Si/Tech(Ker), Pronab Jyoti Nath,Si(Assam), Santosh Tamta, ASI(Chhattisgarh), Abdul Waseem Khan, Si(Delhi), Nilotpal Kumar, Si/Exe, CISF, Tribhuvan Sharma, Si/Exe, CISF, Amit Kumar Sengar, Si/Exe, CISF, Sanjeev Jaglan, SI, SSB, Umesh, Si/Exe, CISF, Prasanta Kumar Pattnaik, ASI(Odisha), C.Sujith, Si/Exe, CISF.

Standing 3 (L to R) S/Sri :- Pintu Sikdar, ASI/WB, Mrityunjoy Mondal,SI(WB),Prasanna Das,SI(Tripura),G.Durga Rao, ASI(AP),K.Ravi Naik, BSI(AP),Asif Iqubal,TO, NTRO, Lt.Col.Mithun.B Sawant(Retd),Asstt.Dir, NTRO.

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on " Sensitization Of New Criminal Laws-2023"

05-08-2024 to 09-08-2024

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on " Handling CCTV Footages & DVR Forensics"

19-08-2024 to 23-08-2024

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on " Introduction & Investigation of AI, Crypto Currency & Block Chain Dark web Transactions"

26-08-2024 to 30-08-2024

CENTRAL DETECTIVE TRAINING INSTITUTE, HYDERABAD

Course on " Introduction & Investigation of AI, Crypto Currency & Block Chain Dark web Transactions"

02-09-2024 to 06-09-2024

CENTRAL DETECTIVE TRAINING INSTITUTE, HYDERABAD

Course on " TOT for IO's In New Criminal Laws"

09-09-2024 to 11-09-2024

CENTRAL DETECTIVE TRAINING INSTITUTE, HYDERABAD

Course on " Sensitization of New Criminal Laws-2023"

23-09-2024 to 27-09-2024

ACTIVITIES AT CDTI, HYDERABAD

1. Conducted an Awareness Program on "Sensitization of New Criminal Laws - 2023" at Osmania University Science College on 05.07.2024. 350 students/ teaching staff have participated.

2. Conducted Awareness Program on Cyber Crimes for the students of Kranthi Degree College, Ramanthapur, Hyderabad on 31.07.2024. 56 students/ teaching staff have participated.

3. Shri. Ramu, Scientist - E, CDAC - Hyderabad visited CDTI, Hyderabad regarding TMIS and took a session to collect suggestions/ feedback from currently undergoing trainees.

4. Conducted Sampark Sabha with the staff of CDTI, Hyderabad on 12.08.2024.

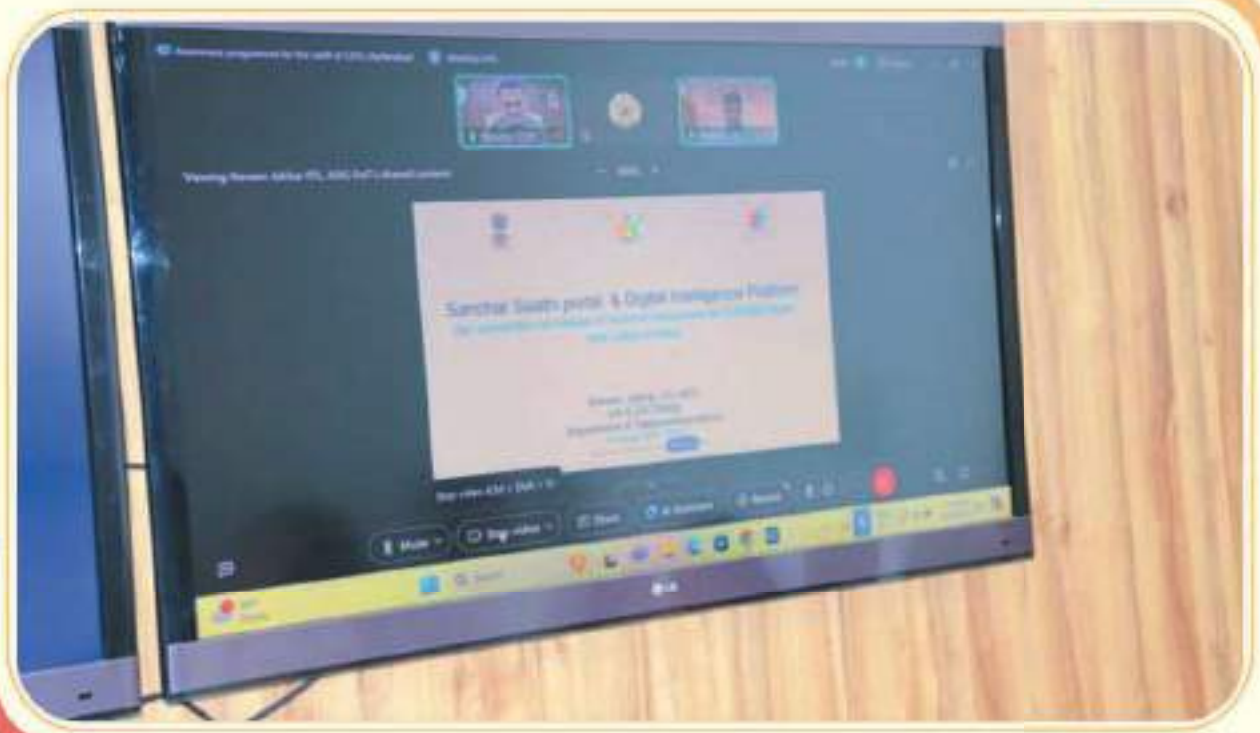
5. (i) Shri. Rajeev Kumar Sharma, IPS, DG, BPR&D visited CDTI, Hyderabad on 13.08.2024 and interacted with the staff. Further he released Horizon magazine for the period Apr - Jun, 24; inaugurated volleyball court; planted sapling in orchard area.

(ii) Conducted awareness program on 'Cyber and social media crimes - how to prevent them' for the XI & XII students of Kendriya Vidyalaya No.1, Hyderabad on 13.08.2024. 108 students/ teaching staff have participated. Shri. Rajeev Kumar Sharma, IPS, DG, BPR&D interacted with students

6. The 78th Independence Day was celebrated at CDTI, Hyd on 15.08.24. Sh Rajashekara N,IPS, Director hoisted flag, distributed the Appreciation letters to guest faculties Sh. Sandeep Mudalkar, Sh. Sridhar M for their contribution in training and program followed by volleyball match.

7. Conducted Advocacy Programme on Competition Law & Public Procurement on 16.08.2024 for the staff of CDTI, Hyderabad by Shri. R C Kumar, Resource Person; Smt. Varalakshmi, Course Coordinator of Competition Commission of India, Telangana.

8. Conducted an awareness meeting with Shri. Naveen Jakhar, Asst. DG, Department of Telecommunications regarding Sanchar Sathi portal and Digital Intelligence Platform on 20.08.2024 for the staff of CDTI, Hyderabad.



9. Sh. Srinivas, SP, CoE, CID and Ms. Sita Reddy, DSP, CoE, CID of Telangana State visited CDTI, Hyderabad on 11.09.2024 and gave presentation on New Verticals in Police Station Created for Investigators, CCTNS using APIs and Centre of Excellence established in Police Headquarters.

10. Conducted a virtual meeting with the team of CDAC, Hyderabad on 12.09.2024 regarding MoU between CDTI, Hyderabad and CDAC Hyderabad on the topics Block Chain Technology, Dark web and Vikaspedia.

11. Various events were conducted to the staff and families on the eve of Raising day of CDTI, Hyderabad on 30.09.2024 & 29.09.2024.

12. On September 20, 2024, an Awareness Programme on 'Cyber Stalking/Bullying and Crimes Against Women and Children' was conducted for students of St. Joseph High School, Gokhale Nagar, Hyderabad. The event drew participation from 150 students and 4 teaching staff. Shri. Rajeev Kumar Sharma, IPS, DG, BPR&D visited CDTI, Hyderabad on 20-09-2024 along with Shri Hemant Priyadarshy, IPS, DGP (Cybercrime), Rajasthan. They interacted with students of St. Joseph's High School, Ramanthapur, Hyderabad for whom an Awareness Programme was arranged

FORENSIC INVESTIGATION OF CRYPTOCURRENCY FRAUD: CASE STUDY OF A DIGITAL HEIST

Sh. Sridhar Mateti,
Cyber Forensic Expert
Guest Faculty

Introduction

In the era of digital currencies, the rise of cryptocurrency fraud has posed unprecedented challenges to law enforcement agencies and cybersecurity experts. This case study delves into a complex forensic investigation of a cryptocurrency fraud, exploring the methods, tools, and challenges faced by investigators in uncovering the perpetrators behind a sophisticated digital heist.

The Cryptocurrency Fraud Incident

In January 2023, a major cryptocurrency exchange reported a significant breach in its security systems. The incident involved the unauthorized access and transfer of millions of dollars' worth of various cryptocurrencies, including Bitcoin, Ethereum, and Ripple. The scale and sophistication of the attack prompted an immediate response from law enforcement agencies and cybersecurity experts.

Initial Incident Response

Identification of the Breach:

The first step in the forensic investigation was to identify the extent and nature of the breach. The cybersecurity team detected unusual activities in the exchange's transaction logs, indicating unauthorized access to user wallets and the movement of funds.

Isolation of Compromised Systems:

To prevent further damage, the compromised systems were isolated. This involved temporarily taking the affected servers offline to preserve their current state for forensic analysis while ensuring the continued operation of other parts of the exchange.

Digital Forensics: Tracing the Digital Footprints

Disk Imaging and Memory Analysis:

Forensic investigators conducted disk imaging of the affected servers and analysed the volatile memory to capture a snapshot of the system at the time of the breach. This process aimed to identify any malware, unauthorized processes, or signs of exploitation in the server's memory.

Timeline Reconstruction:

By analysing logs and timestamps, investigators reconstructed a timeline of events leading up to and during the breach. This step was crucial in understanding how the attackers gained access, moved laterally within the system, and covered their tracks.

User and Access Analysis

Examining user activity logs, investigators identified compromised accounts and traced the unauthorized access points. This analysis involved understanding the methods used by the attackers to obtain login credentials and exploit vulnerabilities within the cryptocurrency exchange platform.

Cryptocurrency Transaction Analysis:

Tracing Stolen Funds on the Blockchain:

Cryptocurrency transactions leave a public and immutable trail on the block--chain. Investigators utilized blockchain analysis tools to trace the movement of stolen funds across various wallets. This involved identifying the wallet addresses used by the attackers and tracking their transactions in real-time.

Exchange Coordination

Collaborating with other cryptocurrency exchanges and law enforcement agencies, the compromised company shared information about the wallet addresses involved in the fraud. This exchange of information facilitated a coordinated effort to freeze assets and prevent the further laundering of stolen cryptocurrencies.

Challenges in the Investigation

Cryptocurrency Anonymity

Cryptocurrencies are known for their pseudonymous nature. The challenge of unmasking the true identities behind wallet addresses required advanced techniques, including collaboration with cryptocurrency exchanges to implement know-your-customer (KYC) protocols.

Cross-Border Legal Challenges:

Cryptocurrency fraud often spans multiple jurisdictions. Coordinating legal efforts across borders to apprehend suspects and recover stolen funds presented a significant challenge, requiring collaboration with international law enforcement agencies.

Legal Proceedings and Arrests

Identification and Issuance of Warrants

Based on the forensic findings, law enforcement agencies identified individuals associated with the cryptocurrency fraud. Warrants were issued for their arrest, and legal proceedings were initiated to bring the perpetrators to justice.

Asset Recovery and Restitution

Simultaneously, efforts were made to freeze and recover stolen assets. Cryptocurrencies were traced to various accounts and wallets, and court orders were obtained to seize these assets for eventual restitution to the affected users.

Lessons Learned and Recommendations

Enhanced Security Measures

The investigation underscored the importance of robust cybersecurity measures. The compromised company implemented enhanced security protocols, including multi-factor authentication, intrusion detection systems, and regular security audits.

User Education and Awareness

To mitigate the risk of social engineering attacks, the compromised company launched a comprehensive user education program. Users were educated about the importance of secure password practices, recognizing phishing attempts, and enabling additional security features.

Conclusion

The forensic investigation of the cryptocurrency fraud exemplifies the complexities involved in unravelling digital heists in the realm of decentralized currencies. Through a combination of digital forensics, blockchain analysis, and psychological profiling, investigators were able to trace the stolen funds, identify the perpetrators, and initiate legal proceedings. This case study highlights the evolving nature of cyber threats and the need for continuous innovation in cybersecurity practices to safeguard the integrity of digital assets in an interconnected world.

THE DARK SIDE OF CONVENIENCE: EXPOSING THE THREAT OF FAKE LOAN APPS

Sh. Aditya Ojha,
Cyber Expert
Guest Faculty

In a world where financial services have never been more accessible, the rise of digital loan apps offers unparalleled convenience. With just a few taps on a smartphone, you can apply for a loan, track your payments, and manage your finances — all without ever stepping foot in a bank. But alongside this convenience lies a growing menace: **fake loan apps.**

These fraudulent applications disguise themselves as legitimate services but are designed to exploit unsuspecting users. The impact can be devastating, leaving victims with compromised personal information, drained bank accounts, and a mounting sense of betrayal. Understanding how to identify and protect yourself from these scams is crucial in today's digital age.

The Appeal of Fake Loan Apps

Fake loan apps thrive by preying on people's need for quick cash. Whether it's for an emergency expense or just to make ends meet, the promise of instant money with minimal hassle can be alluring. Scammers exploit this urgency by creating apps that appear legitimate, often mimicking real financial institutions or using enticing marketing tactics that promise easy approval, no background checks, and low interest rates.
For many users, the urgency to access funds quickly outweighs the need for caution. And that's where the danger begins.

The Tactics Behind Fake Loan Apps

Fake loan apps are designed to mimic legitimate loan platforms, offering users false promises of quick cash. Here are some common tactics used by fake loan apps to deceive users:

1.Too-Good-to-Be-True Offers: They promise unrealistically low interest rates, high loan amounts with minimal documentation, or instant approval with no credit check.

2.Upfront Fees: These apps often demand a "processing fee" or "advance payment" before disbursing the loan. Once paid, the loan never materializes, and the scammers vanish.

3.Data Harvesting and Privacy Invasion: Many fake loan apps request excessive permissions, such as access to contacts, SMS, or personal files, which can lead to the misuse of private data or harassment.

BLACKMAILING IS THEIR MAIN TACTIC

- The accused created 10 WhatsApp groups with people in the contact list and other defaulters as members
- They started posting abusive messages against the defaulters using their photo

- A penalty of ₹3,000 per day was imposed for delayed payment
- The accused started sending morphed photos of the complainant and his mother terming them as fraudsters and cheats, to the people in his phone contacts list. ₹24,000 interest was charged in one week's time on the principal of ₹30,000

Fake Loan Apps: Case Study and Real-World Examples

Fake loan apps come in various forms, but they all follow a similar pattern of deception. Here's a real-world example of how these apps operate:

Case Study: "FastCash Loan"

A fake loan app called "FastCash Loan" promised instant loans with no credit checks and low-interest rates. Upon installation, it requested permissions to access contacts and SMS. After collecting sensitive information, the app demanded an upfront processing fee. When users refused to pay, the app's operators harassed them by contacting their friends and family via the contacts harvested from the app.

Through APK Static Analysis, the app's APK was decompiled, revealing hardcoded URLs that led to suspicious servers located in foreign countries. Further Android App Static Analysis showed the use of obfuscation and malicious scripts that harvested contact lists and financial data. After a widespread complaint from users, the app was removed from the Google Play Store.

The Dangers Lurking Behind Fake Loan Apps

While a genuine loan app operates with clear terms and transparent business practices, fake loan apps are often riddled with red flags. Here's how they pose a threat:

1. Personal Data Theft: When users submit their personal information — such as their name, address, social security number, and banking details — these apps collect and misuse it. Scammers may sell this data on the dark web, leading to identity theft and unauthorized access to bank accounts.

2. Financial Exploitation: Once victims are hooked, these apps may require upfront fees under the guise of "processing" or "insurance" payments. Users, desperate to secure their loan, send money, but never receive the promised funds in return.

3. Unrealistic Loan Terms: Some fake apps may actually grant loans but at extremely high interest rates, hidden fees, or terms that trap users in cycles of debt. Once you fall behind on payments, these scammers turn to harassment, intimidation, and even threats.

4. Malware Installation: In more tech-savvy scams, simply downloading the app can infect your device with malware. This malicious software can monitor your activity, steal sensitive information, and grant hackers control over your phone.

How to Spot a Fake Loan App

With these dangers lurking, it's important to know how to spot a fake loan app before falling victim. Agile Loan app, Apple cash app, Betwinner betting, Bharat Cash, Buddy Loan, Cash Advance, Cash curry, Cash Go, Cash Papa are some of the fake apps.

1. Lack of a Verified Website: Legitimate loan companies almost always have an official, verifiable website that matches the app. If you can't find any information about the app outside of the app store, consider it a red flag.
2. Pressure for Quick Decisions: Fake loan apps often push users to make quick decisions, pressuring them to apply and provide personal information before they can thoroughly review the loan terms.
3. No Regulatory Approval: Every financial institution is typically regulated by a government body. If a loan app is not registered with relevant financial authorities or lacks transparency on this front, it's likely a scam.
4. Unrealistic Offers: Be wary of apps that offer loans without proper documentation, credit checks, or a clear repayment plan. If it sounds too good to be true, it probably is.
5. User Reviews and Ratings: Always read through user reviews before downloading any financial app. While fake reviews exist, legitimate complaints often surface quickly. Pay attention to negative feedback about hidden fees, scams, or unfulfilled promises.

Protecting Yourself From Fake Loan Apps

Staying safe from fake loan apps is all about diligence and awareness. Here are some steps you can take:

1. Research Thoroughly: Before downloading any loan app, do a quick online search about the company. Check for official websites, regulatory approval, and reviews from independent sources. If an app doesn't have a strong digital presence outside of app stores, that's a red flag.
2. Only Download From Trusted Sources: Stick to downloading apps from official app stores like Google Play or Apple's App Store, as these platforms have strict security measures. Even then, look for verified apps from reputable developers.
3. Avoid Unsolicited Offers: If you receive messages, emails, or ads promoting a loan app, proceed with caution. Scammers often use spam tactics to lure people into downloading fake apps. Always initiate contact with lenders through their official channels.
4. Be Skeptical of Upfront Payments: Legitimate lenders will never ask for an upfront payment to process a loan. If you're asked to transfer money before receiving your loan, walk away.

5. Keep Your Devices Secure: Always keep your phone's software up to date and install a reputable security app to protect against malware. This way, even if you accidentally download a malicious app, your device will have an added layer of protection.

What to Do if You Fall Victim:

swift action is key: Report to **1930** & **www.cybercrime.gov.in**

1. Uninstall the App Immediately: Remove the app from your phone to prevent further damage or data collection.

2. Change Passwords: Update all passwords related to your bank accounts, email, and any other sensitive apps on your device.

3. Report the Scam: Contact your bank to flag suspicious activity and report the fraud to the relevant authorities. This may include filing a report with the police and notifying your country's financial regulatory body.

4. Monitor Your Credit: Keep a close eye on your credit score and financial statements for any unusual activity. If your personal information has been compromised, consider freezing your credit or signing up for identity theft protection.

Conclusion:

Fake loan apps are a growing threat in today's fast-paced digital world. They prey on those seeking quick financial solutions, disguising themselves as legitimate services while plotting to exploit your trust. By staying informed, cautious, and aware of the warning signs, you can avoid falling victim to these deceptive schemes and protect both your financial well-being and personal information.

The next time you're in need of a loan, remember: convenience should never come at the cost of security. Take a moment to pause, research, and ensure that the app you trust with your finances is as legitimate as it claims to be.

ANALYZING A PHISHING LINK: A COMPREHENSIVE TECHNICAL APPROACH

Shri. Lakhan Handebag
Cyber Threat Expert,
NCRI&CB, I4C

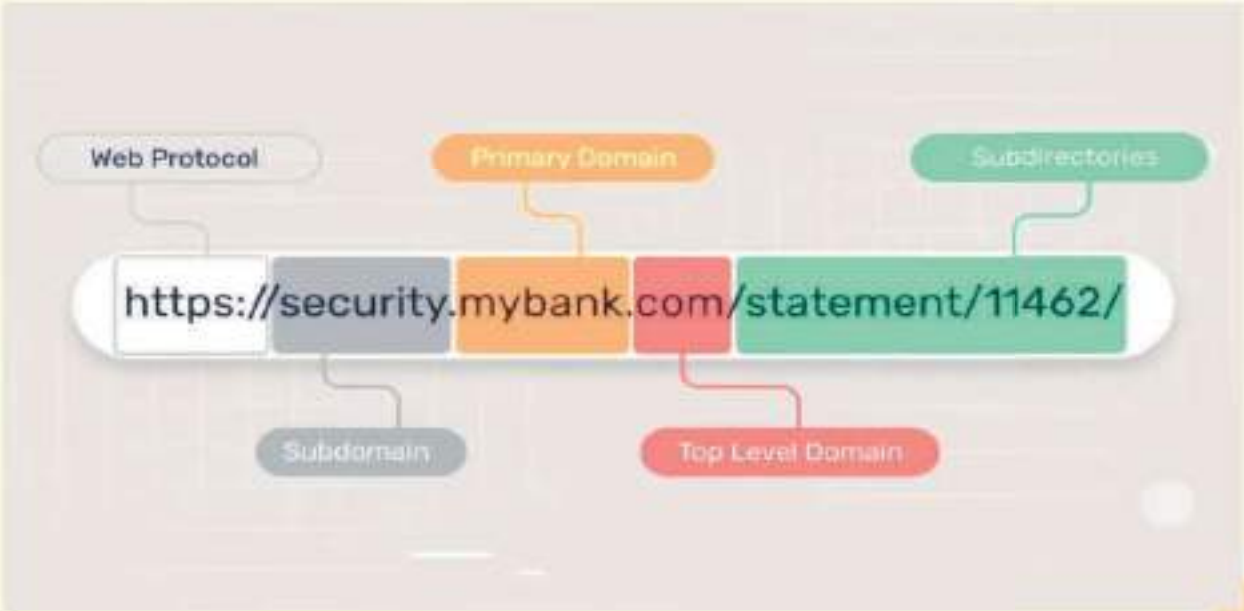
Introduction:

Phishing attacks have grown increasingly sophisticated, often using deceptive links to lure victims into exposing sensitive information or downloading malicious software. To stay ahead of these threats, cybersecurity professionals must be adept at analyzing phishing links to mitigate potential damage. This article delves into both static and dynamic analysis techniques, with a special focus on leveraging VirusTotal for assessing the legitimacy and safety of URLs.

Understanding the Anatomy of a Phishing Link:

Phishing links are crafted to resemble legitimate URLs but contain subtle alterations designed to deceive users. Before diving into deeper technical analysis, it's essential to recognize these characteristics:

- *Top-Level Domain (TLD):* Attackers often use lookalike domains such as "g00gle.com" instead of "google.com."
- *Subdomains:* Malicious links might hide behind seemingly valid subdomains, like "login-bank.google.security-check.com."
- *Protocol:* While HTTPS provides encryption, it does not guarantee the safety of the site, as attackers increasingly use SSL certificates.



Initial Inspection of a Phishing Link

Before diving into technical analysis, a quick initial inspection of the URL can often reveal red flags:

- *Misspelled Domains:* Subtle misspellings, like "faceb00k.com" instead of "facebook.com," are common.
- *Query Strings:* Check for unusual query parameters that may be used to track or steal information.
- *Shortened URLs:* Expand shortened URLs with tools like CheckShortURL to see the destination before clicking.

Static Analysis

Static analysis focuses on gathering information from the URL without directly interacting with it.

a) URL Decoding

Attackers often encode phishing URLs to obscure their true destination. Tools like CyberChef can decode these URLs, revealing their actual components.

b) Whois Lookup

Perform a Whois lookup to gather information on domain registration. Key elements to focus on:

- Registration Date: Recently created domains are often used for phishing.
- Registrar: Unknown or suspicious registrars can be a red flag.
- Anonymous Registration: If ownership details are hidden, this may indicate malicious intent.

c) DNS and IP Address Information

Check the DNS records associated with the URL:

- A Records: The IP address linked to the domain.
- MX Records: If the site manages email, misconfigured records can hint at a phishing operation.
- Reverse IP Lookup: Look for other sites hosted on the same IP, which might reveal further malicious domains.

d) Blacklists and Reputation Check

One of the most powerful tools for static analysis is VirusTotal, which provides an immediate overview of the URL's reputation.

Using VirusTotal for Phishing Link Analysis

VirusTotal is a multi-engine URL and file scanning service that aggregates results from various antivirus solutions and URL scanners. When analysing a phishing link, VirusTotal can offer vital insights on the legitimacy and safety of the URL.

a) Submitting a URL to VirusTotal:

1. Visit VirusTotal's website and submit the phishing URL for analysis.
2. VirusTotal will scan the link with numerous engines (e.g., Google Safe Browsing, PhishTank, Kaspersky).
3. After scanning, VirusTotal will provide an aggregated report, highlighting whether any of the engines have flagged the URL as malicious.

b) Understanding VirusTotal Reports:

Once the scan is complete, VirusTotal generates a report that includes:

- Detection Rate: How many of the scanning engines flagged the URL as malicious.
- URL Categories: VirusTotal categorizes the threat (e.g., phishing, malware).
- Community Comments: These are useful for seeing if other users have encountered the same URL.
- Historical Data: VirusTotal maintains a history of URLs, allowing you to track whether a link has been flagged in the past, even if it was temporarily cleaned.

For example, if a URL is flagged by multiple engines as a phishing site, it can serve as confirmation of its malicious intent. Additionally, VirusTotal can show if the URL redirects to a known malicious site.

Dynamic Analysis

Dynamic analysis involves interacting with the URL in a safe environment to observe its behaviour. This method is particularly useful when a phishing link hasn't been flagged in static checks.

a) Sandboxing

By running the phishing link in a sandbox environment, such as Cuckoo Sandbox or Any.Run, you can observe its behaviour without risking your system. Look for:

- Redirections: Does the link redirect users to different malicious domains?
- JavaScript Execution: Many phishing pages use scripts to steal credentials or install malware.
- Network Activity: Monitor any outbound traffic or connections to Command-and-Control (C2) servers.

b) Traffic Inspection with Burp Suite

Burp Suite is a powerful tool for capturing and analyzing the traffic between your browser and the phishing site. Key elements to check include:

- Form Submissions: See where the page submits sensitive data, such as passwords or personal details.
- SSL/TLS Handshake: Malicious sites may have self-signed or misconfigured certificates.

Payload and Malware Analysis

Phishing links often deliver malicious payloads, such as malware or ransomware. If the link downloads a file, it is crucial to analyze the payload.

- *File Hash Check*: Upload the downloaded file to VirusTotal to check if the file hash matches any known malware samples.
- *Disassemble the Code:* Use tools like IDA Pro or Ghidra to reverse-engineer the file, revealing its functionality.
- *Behavioural Analysis:* Run the file in a sandbox to observe any malicious activities it performs, such as keylogging or data exfiltration.

PeStudio – Process Hacker – ProcMon – ProcDot – Autoruns – Fiddler – Wireshark – X64dbg – Ghidra – Radare2 – Cuckoo Sandbox

Indicators of Compromise (IoCs):
Hash values related to malicious files – Malicious software and code – Dangerous IP addresses – Digital footprint or indicator of an attacker's work

Throughout your analysis, document key indicators of compromise, including:
- Domain Names: Malicious or suspicious domains.
- IP Addresses: Associated with phishing campaigns or other malicious activity.
- File Hashes: For malware that may have been downloaded.
- Redirection Chains: The path a phishing link follows, which may include multiple malicious domains.

These IoCs are essential for network defense and can be used to block phishing attempts and identify similar attacks in the future.

Conclusion
Phishing links present a significant threat in today's cybersecurity landscape, requiring thorough analysis to fully understand their potential impact. By employing a combination of static analysis, dynamic sandboxing, and leveraging powerful tools like VirusTotal, cybersecurity professionals can dissect and mitigate the risks associated with phishing links. VirusTotal, in particular, offers an indispensable tool for quickly assessing the reputation of a URL, while sandboxing and traffic inspection provide deeper insights into the malicious behaviour hidden beneath the surface.

Through vigilance and a methodical approach, phishing attacks can be identified and neutralized before they result in significant damage.

PROTECTING CHILDREN'S DIGITAL PRIVACY: A GROWING CHALLENGE

Smt. Anusuya Baral,
Dy. SP, CDTI, Hyd

The digital age has transformed the way children interact with the world, offering unprecedented access to information and opportunities for learning and growth. However, this digital landscape also presents significant risks to children's privacy. As technology continues to evolve rapidly, it becomes increasingly imperative to safeguard children's personal information and protect them from online threats.

The Digital Landscape and Children:

Children are increasingly immersed in the digital world. They use smartphones, tablets, and computers to access a vast array of online content, including social media platforms, gaming apps, educational resources, and entertainment websites. While these technologies offer numerous benefits, they also expose children to potential dangers, such as cyberbullying, exposure to inappropriate content, and privacy breaches.

Key Privacy Concerns for Children:

Data Collection and Tracking: Many websites and apps collect a significant amount of personal information about children, including their names, addresses, browsing history, and online activities. This data can be used for targeted advertising, behavioural tracking, and even sold to third-party companies.

Cyberbullying and Online Harassment: The anonymity and reach of the internet can make it easier for children to be bullied or harassed online. This can have severe emotional and psychological consequences.

Exposure to Inappropriate Content: Children may accidentally or intentionally encounter inappropriate content online, such as violent, sexually suggestive, or harmful material. This can be distressing and damaging to their development.

Privacy Violations: Children may inadvertently share personal information online, such as their location, photos, or contact details. This can lead to privacy breaches and potential risks.

Strategies for Protecting Children's Digital Privacy

Parental Controls and Monitoring: Parents can use parental control settings on devices and internet service providers to restrict access to certain websites, apps, and content. They can also monitor their children's online activities to ensure their safety and privacy.

Open Communication and Education: Parents should have open and honest conversations with their children about online safety and privacy. They can educate them about the risks of sharing personal information, the importance of strong passwords, and the consequences of engaging in harmful online behaviours.

Privacy-Focused Technology: There are a growing number of privacy-focused technologies and services available for children. Parents can consider using these tools to protect their children's online privacy.

Awareness and Advocacy: Raising awareness about the importance of protecting children's digital privacy is crucial. Parents, educators, and policymakers can advocate for stronger privacy laws and regulations to safeguard children's personal information.

Empowering Children: Children should be empowered to make informed decisions about their online activities. They can be taught to be critical consumers of information and to be mindful of their privacy settings.

Verifiable Consent: A New Standard for Parental Approval

Verifiable consent is a method that ensures parents or guardians give explicit permission for their children to engage with digital services. Traditional consent mechanisms, such as simple checkbox agreements, often fail to ensure that parents are genuinely aware of what they are consenting to. This inadequacy can lead to a false sense of security regarding children's data privacy.

To enhance the efficacy of consent processes, verifiable consent frameworks utilize technologies that authenticate the identity of parents or guardians. For instance, services could implement two-factor authentication or biometric verification (like facial recognition) to confirm that the person providing consent is indeed the child's parent. This creates a more robust consent mechanism that reduces the likelihood of unauthorized access.

Furthermore, platforms could provide clear, comprehensible information about what data will be collected and how it will be used, enabling parents to make informed decisions. By establishing verifiable consent as a standard practice, digital platforms can better protect children's data while ensuring parents are actively involved in their child's online activities.

KYC-Based Age Verification: Ensuring a Safer Digital Environment

KYC-based age verification is another vital approach to protecting children online. This method involves verifying the identity and age of users before granting access to certain platforms or services. It aims to ensure that children are only exposed to age-appropriate content and are not subjected to environments that may be harmful or exploitative.

Implementing KYC processes typically involves collecting information such as government-issued IDs, biometric data, or even parental verification to confirm a user's age. While this raises concerns about privacy and data security, innovative solutions are emerging that balance these needs. For example, some systems allow users to verify their age without retaining sensitive information, using cryptographic techniques to ensure data is not stored or misused.

Moreover, KYC-based age verification can help platforms comply with regulations such as the Children's Online Privacy Protection Act (COPPA) in the United States and similar laws worldwide. By ensuring that users are of the appropriate age, platforms can protect themselves legally while fostering a safer online environment for children.

Challenges and Considerations

1 in 6 parents don't use parental controls – 39% of parents don't have time to monitor their children's social media usage – 21% of parents can't find information to set up monitoring – 32% of children find ways to circumvent parental controls

While verifiable consent and KYC-based age verification hold great promise, they are not without challenges. Concerns regarding user privacy, data security, and potential barriers to access must be carefully considered. Implementing robust systems can be costly and complex, particularly for smaller companies and startups. Additionally, there is a risk that overly stringent verification processes may inadvertently exclude children from beneficial online resources.

To address these issues, stakeholders—including policymakers, tech companies, and child advocacy groups—must collaborate to create comprehensive frameworks that protect children's digital privacy while ensuring accessibility. Continuous education for parents, children, and educators about online safety and privacy is also crucial.

IMPLEMENTATION OF FUNCTIONAL VERTICAL SYSTEM IN TELANGANA STATE

Smt. Sita Reddy,
Dy.SP - CoE,
CID, Telangana

A unique initiative is implemented in Telangana State Police for rendering Quality services to the citizen/community and to ensure safety, security of the people at all levels. This initiative makes the TS Police robust ensuring quality and accountability in services rendered to citizen, strengthening the staff working at grass root level, enhancing their caliber and targeting Uniform Service delivery to common man.

To Systematize, Standardize and Institutionalize the work culture of Police in Telangana State a system of **"Functional Vertical"** has been established in the 2018. This initiative aims to enhance the functional abilities of all officers and personnel, ensuring the delivery of 'Quality' and 'Uniformity' in services rendered and the creation of an effective, efficient mechanism to safeguard the safety and security of people. And also to maintain standards of performance at police station level through a system driven approach where processes are well designed, irrespective of the priorities of the SHO.

In accordance with this objective, the Government of Telangana issued order vide GO.MS. No. 31, of HOME (LEGAL) DEPARTMENT dt: July 21, 2022. The work at the police stations is identified & divided into **17 Functional Verticles,** each having its own well defined work processes, techniques, deliverables, time lines, Key performance indicators (KPI) etc.

A Functional Vertical is a role or work that is being performed by an individual at the PS level which is measurable through KPIs. **KPIs** are predetermined, measurable indictors which are given weightage according to their importance and are communicated to role performer and measured in real time.

The Key Objectives of initiating Functional Verticals Structure are mentioned below:

- ❖ Division of Work
- ❖ Role Clarity
- ❖ Empowerment
- ❖ Role based Capacity Building activities for enhancement of professional, soft and technical skills
- ❖ Functional Specialization
- ❖ Work Measurement and accountability
- ❖ Proactive Policing through ownership

- Motivation through performance based Rewards & Recognition
- Strengthening citizen centric service delivery mechanism through uniform service delivery and friendly policing for better co-operation and coordination among stakeholders.
- For better analyzation, strategy preparation and implementation of evidence based policing.

The List of (17) Functional Verticals (roles) that are being performed at PS level are mentioned below:

1. Reception - First point of contact for the public visiting the Police station
2. Station Writer - Maintains the Police station records
3. Crime Writer - Maintains the records of crime and criminals
4. Blue Colts - Keeps vigil round the clock and reach instantly to any spot of distress
5. Patrol Cars - Responsible for enforcing law and responding to the emergencies for maintenance of Peace & Order.
6. Court Work – Keeping the records, pursuing of all the Court cases duly coordinating & assisting all stakeholders
7. Warrant Issue - Responsible for the execution of the criminal warrants and other documents of arrest
8. Summons service - Maintains the records of the summons received, served, pending, returned etc.
9. Tech Team - Responsible for overall supervision and control of technology used by the department
10. Investigation (All IOs) - Developing process, tools, techniques etc., for collection of evidence to substantiate and prove the facts.
11. Crime Teams - Responsible for keeping surveillance, prevention & detection of all property offences.
12. Medical Certificates – Collection of Medical Certificates, expert opinions and maintenance of records.
13. Section In-charge - Responsible for Coordination of Functional Verticals in attending to all Dial 100 & Emergency Calls and in other operational duties
14. Sector SI – Conducting petition enquiries, Community Policing, Crime Prevention, Investigation, Criminal Surveillance & maintaining peace & order in his AOR.
15. Detective Inspectors (DIs) - Responsible for surveillance, crime prevention, detection, investigation and supervising of trials in all property offences.
16. Sub-Inspector (Administration) - Responsible for Station House Management, technology implementation, PMS etc.
17. Station House Officer (SHO) - SHO is the end owner and responsible for complete deliverables.

CENTER OF EXCELLENCE

To develop, monitor, sustain and maintain this unique initiative of Functional Verticals a special unit called Center of Excellence was established at the State Headquarters at Hyderabad to ensure "Uniformity in Service Delivery" to the citizen. Hence, the role and purpose of CoE is to be the Key Driver of organizational Change in all functional verticals.

CoE strives for continual improvement in service delivery standards and functional verticals at the PS level.

The COE was tasked to:

- Define the FV roles
- Design Standard Operating Procedures (SOPs)
- Determine Key Performance Indicators (KPIs)
- Impart Training to FV teams vertical-wise
- Provide IT resources, tools and infrastructure
- Track and measure Performance against KPIs and feedback
- Reward and Recognize Best Performance at all levels

Performance assessment of the personnel:

The performance of every individual working at the field is assessed, measured every month through Key Performance Indicator (KPIs). KPI based performance measurement has brought about responsibility, accountability and transparency into Police work. A process based approach through the efforts of all the functional verticals has resulted, yielded significant results in Telangana State Police.

The performance of every individual is measured and assessed every month across all 747 police stations of TS while the data is retrieved from 16 applications. (Data is filled by role performer during the course of their duty) and is analyzed basing on the KPIs (Key performance Indicator) of each Functional Vertical. Regular performance feedback is also given to the employees.

The Quality of services is also ensured by checks, the gaps/lacunae resulting in poor performance are evaluated and necessary Capacity Building trainings are organized to personnel to enhance their capacities in that concerned role.

Benefits of FV system:

- Increased workforce accountability
- Enhanced lateral co-ordination
- Increased functional Expertise
- Breaking the workflows soils
- Rapid information and communication flow
- Empowered teams and Employee engagements
- Internally, there would be a radical paradigm shift that is likely to be created when organizational restructuring of this nature is attempted across the organization
- Self-motivated, well-defined role clarity, specialized expertise.
- Higher engagement levels.
- Optimal performance and team synergy and energy levels.
- Leadership role for every Station House officer (SHO) –strengthen.
- SHO to become a strong link in the organization.
- Team development and breaking of silos.
- Increased empowerment and reduced dependency on the top.
- High level motivation and involvement from every employee as the system is transparent and output-driven.

- Crime Reduction (Snatchings, Kidnaps, Robbery,)
- Detection and Recovery
- Reduced Response Time (10 mins)
- Increased Visible Policing
- Improvement in Citizen Centric Services (PMS, Mee-Seva, Online Citizen Portal)
- Reward and Recognitions for Police Personnel
- Enforcement of law and reduction of accidents

Results achieved in Telangana state after implementation of this Functional Vertical System

★ Accountability and responsibility
★ Enhanced performance
★ Improved positive Image of Police
★ Awards and rewards
★ Training and professional development
★ Community involvement
★ Crime reduction (snatchings, kidnaps, robbery)
★ Convictions improvement
★ Detection and recovery of property offenses
★ Reduced response time (10 mins)
★ Increased visible policing
★ Improvement in citizen centric services (PMS, Mee-seva, Online citizen portal)

Conclusion:

The Functional vertical System has brought about a path breaking transformation in TS Police into SMART Police, setting a benchmarking standards of safety and security, in the field of policing. Even though it is in the transitional stage of implementation across the state in all functions, the results are indicative of some significant qualitative and quantitative results towards positive direction and also enhancing the image of the Police. TS Police, in its endeavor to bring in development in policing services, has introduced an intervention of restructuring its core police functions into different Functional Verticals with an intention to utilize talent and potential of personnel to optimal levels.

The FV system and the KPI based measurement has brought about responsibility, ownership, accountability and transparency into police work and also in the services rendered to the citizen.

It is beyond doubt that the Functional Verticals and Centre of Excellence has infused dynamism into the operational ecosystem in-tune with the changing environment. The cascading effect of initiating Functional Verticals in the Police structure leading to the ultimate organizational excellence on a sustainable basis beyond individual person-driven leadership is visible and is a compelling promise to its future.

USES OF DRONES IN CRIME ANALYSIS

Shri. Rajashekara N, IPS
DIG/Director,
CDTI, Hyderabad

Drones, also known as Unmanned Aerial Vehicles (UAVs), have revolutionized several industries, including law enforcement. Their ability to fly, gather data, and perform multiple functions with minimal human involvement makes them an invaluable asset in modern crime analysis and forensic investigations. From crime scene documentation to surveillance, drones provide law enforcement with a new perspective on criminal activity and investigation procedures. Their applications span across various sectors like crime scene analysis, military operations, border security, VIP protection, and disaster response, all of which will be discussed in detail.

Drones Functioning

Drones perform two primary tasks: flying and navigation. These activities are made possible by several key components:

1. *Power Source:* battery or fuel for power.
2. *Rotor Blades and Propellers:* helps to maintain flight.
3. *Lightweight Frame:* Made of composite material, this helps maximize speed and reduce weight.
4. *Remote Controller:* This connects to the drone via Wi-Fi or other radio waves, allowing the user to control the drone's movement.

Anatomy of Drones

There are different types of drones, each serving a specific purpose:

1. *Multi-rotor Drones:* Often used for surveillance and photography.
2. *Single-rotor Helicopters:* Known for better flight efficiency.
3. *Fixed-wing Drones:* Used for longer-duration flights.
4. *Hybrid VTOL (Vertical Take-off and Landing):* Combines the best features of multi-rotor and fixed-wing designs.
5. *Drone Controllers:* Essential for flight and navigation.

Crime Scene Documentation with Drones

Drones offer aerial perspectives that provide a comprehensive view of crime scenes. They can capture high-resolution images and videos that reveal critical evidence often missed by ground-level investigators.8

- *3D Mapping:* Equipped with LiDAR (Light Detection and Ranging), drones can create 3D maps that assist in accident reconstruction and provide a detailed understanding of the crime scene layout.

• *Evidence Location:* Drones can locate evidence that may be hidden or obscured in places that are difficult to reach, such as rooftops or dense vegetation.
• *Crime Scene Reconstruction:* By capturing footage from multiple angles, drones help law enforcement reconstruct events and gather critical details.

Search and Rescue Operations:

Drones are valuable in search and rescue operations, especially in remote or dangerous areas where ground access is limited. Equipped with thermal cameras, they can detect heat signatures, aiding in locating missing persons or suspects during nighttime operations or in hard-to-reach locations.

Key Advantages of Using Drones in Crime Scene Investigation

• *Rapid Deployment:* Even to increasable points or SOC drones can be sent.
• *Comprehensive Overview:* They provide a broad layout of the crime scene, helping investigators identify key evidence.
• *Evidence Preservation:* By reducing human interference, drones minimize contamination of the crime scene.
• *Time-lapse Photography:* Drones can capture time-lapse sequences, allowing law enforcement to track changes in the scene over time.

Military Operations and Warfare

1. Targeted Strikes: Drones can perform precision strikes on high-value targets with minimal collateral damage.
2. Close Air Support: Drones provide real-time targeting support to ground troops, enhancing combat effectiveness.
3. Logistics and Resupply: Drones can transport medical supplies, food, and equipment to remote areas.
4. Electronic Warfare: Some drones can disrupt enemy communication and radar systems.
5. Psychological Operations: The mere presence of drones can have a significant psychological impact on enemy forces, deterring hostile actions.

VIP Surveillance

Drones are increasingly used for VIP surveillance to enhance security at high-profile events:
1. Real-Time Monitoring: Drones provide live aerial footage, enabling security teams to monitor large crowds and detect potential threats.
2. Crowd Control: Drones help maintain order by monitoring crowd behavior at large events like the G-20 summit and religious gatherings such as Kumbh Mela.
3. Risk Assessment: Drones can assess security risks before events, helping to develop strategic security plans.
4. Access Control: They ensure that only authorized personnel enter restricted areas.

Border Security

Difficult to patrol by foot; like India-Pakistan, India-Bangladesh

1. Real-Time Surveillance: Drones can capture live video and thermal imagery to detect unauthorized border crossings and other suspicious activities.

2. 24/7 Surveillance: With AI-enabled cameras, drones provide continuous monitoring and situational awareness, improving security at borders like the India-Pakistan border.

3. Environmental Monitoring: Drones are also used to monitor environmental changes, such as deforestation or habitat loss, in border areas. Thus it helps the IMS and forms who can forecast the weather

However, drones have also become a preferred tool for illegal activities. For instance, drug traffickers along the U.S.-Mexico border frequently use drones to transport narcotics. Similarly, drones were used by Yemen's Houthi rebels to attack Saudi Aramco oil facilities in 2019, and in 2021, drones were involved in an attack on an Indian Air Force base by suspected Lashkar-e-Taiba terrorists.

Disaster Response:

Seen pictures dropping food packets, conducting aerial survey. Search of air object like plan crash etc

1. Damage Assessment: After natural disasters like floods or earthquakes, drones can quickly assess the damage and provide critical information to first responders.

2. Search and Rescue: Drones can locate survivors trapped in remote or hazardous locations. But often they travel fonter and miss them

3. Aid Delivery: Drones can deliver medical supplies and food to areas that are otherwise inaccessible, during flood, and forest fires

Drone Forensics and Law Enforcement:

1. Beat Patrolling: Drones are integrated into beat patrolling systems, enabling real-time surveillance of specific locations. In future it may replace beat constables

2. Night Vision: Drones equipped with night vision cameras can assist in detecting criminal activities in dark or remote areas. For Naxalite operations in night

3. Evidence Gathering: Drones can capture crucial evidence that might not be available through traditional CCTV footage, especially in high-density areas.

Drone Regulation and No-Fly Zones As per Drone Rules 2021

In India, drone usage is regulated based on geographic zones:

- *Red Zone:* Areas like international airports where drone operations are strictly prohibited without permission from the central government.
- *Yellow Zone:* Includes areas within a certain distance from airports where drone operations require permission from air traffic control.
- *Green Zone:* Areas where drones can operate without requiring special permission, as long as they fly below 400 feet.

Violations of these rules can result in fines, as demonstrated in cities like Gurgaon and Noida, where drones are used for traffic management and law enforcement.

Anti-Drone Technology

To counter the threat posed by rogue or malicious drones, law enforcement agencies are deploying anti-drone technologies:

1. Anti-Drone Guns: These devices can block the communication between a drone and its controller.

2. Laser Systems: Drones can be neutralized using lasers to jam their communication or disable them.

3. Frequency Blocking: Frequencies such as 2.4 GHz and 5.2 GHz, commonly used by drones, can be disrupted using specialized equipment.

Future of Drones in Law Enforcement

The future of drones in law enforcement is promising, with advancements in artificial intelligence (AI) enhancing their functionality. Drones equipped with AI cameras can recognize suspects, monitor traffic, and even raise automated challenges to violators. Law enforcement is increasingly integrating drones into their broader surveillance and intelligence-gathering systems, Conduct recce of the operations.

For instance, in Bangalore, AI-enabled cameras installed at traffic points are already being used to recognize criminal activity like in Bangalore-Mysore Road after the BGS flyover from Bangalore AI enable cameras have identified many criminals. In traffic junctions it can detect suspected criminals, vehicles and report to command control centre. Additionally, drones are being employed in complex operations like hostage situations, border security, and environmental monitoring.

Conclusion

Drones are reshaping the landscape of crime analysis and law enforcement. Their ability to provide real-time surveillance, gather evidence, and assist in critical operations like search and rescue make them indispensable tools. While their use must be regulated to ensure privacy and security, their benefits in improving efficiency and response times are undeniable. As technology evolves, drones will continue to play a crucial role in law enforcement, military operations, border security, and disaster response, making them a vital asset for modern society. Most of the jobs in coming days become techno-oriented and AI enabled tools, drones doing courier work and in traffic places people started moving through drones like present day ola/ uber, thus saving major cost, time and energy.

CENTRAL DETECTIVE TRAINING INSTITUTE HYDERABAD

cdtshyderabad@nic.in cdtihyd@gov.in
040-27038182, 29704150
@bprdcdtihyd
@bprdcdtihyd
@bprdcdtihyd

Address:
CDTI, Ramanthapur,
Hyderabad,Telangana,
Pin-500013

Editor in cheif : Shri Rajashekara N, IPS, DIG/Director
Editor : Smt. Anusuya Baral, Dy SP
Member : Shri. V. Bheemakrishna Naik, PA (Trg.)