Sytech Labs

Strengthening Cyber Security

Private Limited

Sytech Labs : Reinforcing Cyber Security by Predicting and Mitigating Cyber Threats

SANDEEP MUDALKAR
CEO & Founder

"Ethical Hacker Who Fights Against Cyber Crimes"

His Specializations Includes

- Information Security Professional & Researcher
- Vulnerability Research and Disclosure
- Penetration Testing
- Vulnerability Assessment of the Networks & Systems
- Cyber Crime and Forensics Investigator

SECURING PERSONAL DATA

Ensuring Data Privacy through Personal Data Protection Solutions

Organization's Essential Deliberations in managing the Risks to CYBER-WORLD

Over the years, there has been gigantic development in the cyber-world due to the extreme growth in the information technology. But the security of this cyber-world is often exploited and is at risk. Currently, there is a severe threat to very basic and highly confidential data. The security organizations are majorly focusing on cyber-security threats rather than other means of attack/ than any other means of attack. We are presently working on the cutting-edge spying techniques and other methodologies to manage Cyber security risk. The expansion of technology from cell phone to the smartphone has engaged the government to work closely with the private sector to secure the cyber network.

Sharing the Information

The confidential information leaking can bring the stability of an organization into danger. Securing and managing this information is a perfect insight to create a strong base for an organization. The investors must be alert to the risks, predominantly of cross-cutting and shared risks, and be involved in complex decision-making processes. Information sharing should involve appropriate communication processes. These processes must embrace thresholds and criteria for communicating and escalating risks. Tools used for sharing information, such as dashboards of pertinent metrics, can keep investors conscious and involved. Sharing the information helps to identify, asses, and respond to a cyber-security risk and permit risk decisions to be well informed, well considered, and built with a perspective to satisfy organizational objectives.

SYTECH LABS PVT.LTD

Prioritizing Data Security in the Digital Age Enlightening Students & Professionals via Nonpareil Training & Consultancy

With the advancement of technology, the knowledge resources are becoming an open source by boosting students and researchers to learn more about Cyber Security. The new era of Cyber Defense in India has grown to maximum from personal to corporate level, social networking, social media; knowledge sharing websites that are very rapidly growing in securing the people.As security is the major aspect for every nation. The government of India has secured ambitious plans to raise cyber connectivity with various activities related to e-governance and e-commerce that are now being carried out over the Internet.

Sytech Labs Pvt Ltd is one of the leading IT Security Firms in India, that is known for providing business solutions to their clients in terms of training, systems integration, consulting, outsourcing, application development, and networking. Sytech Labs Pvt Ltd services line include Information Security Training, Seminars & Workshops, Cyber Crime Investigation & Consulting, Vulnerability Assessment & Penetration Testing (VA/PT), IT Security Consulting & Auditing, Web Application Development, Search Engine Optimization, Network Solutions etc.

Sytech Labs Pvt Ltd was Founded in year **2014** by Headquartered at Hyderabad **Mr.SANDEEP MUDALKAR - Cyber Crime Investigator & Trainer** with motivation of his father **M.K.Vishwanatham, Deputy Conservator Forest (Rted).** In short span, Sytech Labs Pvt Ltd has improved the infrastructure. Sytech Labs Pvt Ltd has conducted plenty of seminars & workshops for police department and various educational institutes across the India. Our team always cop with Crime Branch Departments of various states for Investigating Cyber Crimes. As the world facing increased number of cyber-crimes, our training department is working hard to deliver best IT Security knowledge to our students to make them best for the IT industries. Our team includes experts from most of the states of the India. Sytech Labs Pvt Ltd Team has helped the society by offering consultancy of cyber laws & cyber-crime investigation for victims. Our qualified team of Software Developers & Web Developers is been always appreciated by our clients for providing them best out of the best Web Solutions.

OBSTACLES FACED AT IGNITION POINT

At the beginning of the journey, while establishing the organization, Sytech Labs faced several difficulties over a year in finding a good team for sorting out issues in their projects and there was also a tough task in forming cyber security expert's team which is very rare especially in India. They also faced multitask Investigation across critical cases from various police department regarding Fake profiles of Social Networking Cases, Credit & Debit Card cloning, Cyber Stalking, Fake Lotteries, Data Integrity, Phishing, Email Hacks, Denial-of-service (DoS), Programming flaws, Spoofing attacks, Virus & Worms in Networks, Website Hacks, Leakage of Private information on blogs etc.

Besides the fact that Internet, the sophisticated creation of mankind, has eased the lives of people through diversified means, it has also evolved into a space posed with proliferating menaces that are incomprehensible even to cyber professionals. Sytech Labs extends its training centre & consultancy to a wide range government organisations in which conducted trainings for on Cyber Security for MCEME, Indian Army, Judges and Public Prosecutor, National Institute of Smart Governance(NISG), Customs and Central Tax, Central Detective Training Instuite(CDTI), MCRHRDI, APHRDI, Cyber Crime Department of Hyderabad and many more on not just modifying their investigation strategy as per the cyber crime case, but also on spreading awareness about the security parameters evolving with technological changes.

SECURED FUTURE OF SYTECH LABS

The cyber threats will certainly pose a significant challenge to IT professionals across all sectors with the increase in technologies such as cognitive computing, and big data analytics. Besides the IoT is further influencing the increasingly connected world in unprecedented ways.

While talking about the future steps that are taken on cybercrimes by the organization,Sandeep states "Our goals is to be one among the best cyber security experts over India, trying hard to get tie-up with various governments across India as there are many flaws in government systems & apart from this we are focusing on M-Commerce & E-Commerce projects etc."

> *" Sytech Labs assures to provide rigorous training to them on promoting security and identifying potential risks like database leakages, system & email hacks and a lot more "*

OFFERINGS :

- ♦ Cyber Crime Investigation & Consulting
- ♦ Information Security Training
- ♦ Seminars & Workshops
- ♦ Vulnerability Assessment & Penetration Testing (VA/PT)
- ♦ IT Security Consulting & Auditing
- ♦ Web Application Development and Auditing
- ♦ Search Engine Optimization
- ♦ Network & Its Penetration Testing

SANDEEP MUDALKAR
FOUNDER & CEO

During his early days of schooling at St. Marys High school in Hyderabad, Sandeep was an ardent follower of technology and science. Participating and winning a few science exhibitions and tech competitions, hi--vs interest was rapidly holding the reins of technology. As the next step, he completed his Bachelor Degree in Electronic & Communication Engineering from the prestigious college from Aurora College, JNTU University where his inclination towards computer science and technology started shaping up. This was the time when Sandeep recognized the necessity of 'Security' in an application, database, code or network, which catapulted him towards Ethical Hacking and motivated him to pillar his career in IT security.

After completing his graduation, Sandeep joined TATA consultancy service as an Network Security Analyst Evangelist and successfully stirred his role of IT Security Trainings for corporate. This volume exposed Sandeep to real-time VAPT projects and contributed in shaping up his professional life at its best.

RENOWNED ETHICAL HACKER & CYBER SECURITY EXPERT

With this substantial amount of experience and good industry contacts, **Mr.Sandeep Mudalkar** established Sytech Labs Pvt Ltd in the year **2014** with the motivation from his father **Mudalkar Kashi Vishwanatham (Deputy Conservator of Forest-Retd)**, family, well-wishers and his wife **Shalini Mudalkar-Co-Founder** and today he is a Cyber Security Trainer, Investigator and Consultant with various government departments, and researcher of cyber security. He was interviewed and participated in live debates by several print and elec-tronic media The Hindu, Deccan Chronicle, The New Indian Express, India Ahead, Zee TV, Zee News(Hindi), TV9, NTV, Eenadu Etharam, T-News,V6, Express TV, CVR News etc. He was even rewarded by IAS & IPS officers for solving complex cases of cyber crimes, identifying bugs in government sites, & helped them to improve security and reowned as Cyber Crime Investigator.

Under the leadership of young entrepreneur Sandeep, the team has always copped up with Crime Branch Departments of various states for Investigating Cyber Crimes. In a short span of time, Sytech Labs has improved the in-frastructure by conducting plenty of seminars & workshops across India. He has also conducted awareness on Cyber Crimes for more than 200+ schools, Intermediate & Degree Colleges & more than 150+ workshops on Ethical Hacking at various engineering colleges where as many students and professionals got benefited by his lectures.

A Zealous IT Security Professional

OBSTACLES FACED AT IGNITION POINT

At the beginning of the journey, while establishing the organization, Sandeep faced several difficulties over a year in finding a good team for sorting out issues in their projects and there was also a tough task in forming cyber security expert's team which is very rare especially in India. They also faced multitask Investigationacross critical cases from various police department regarding Fake profiles of Social Networking Cases, Credit & Debit Card cloning, Cyber Stalking, Fake Lotteries, Data Integrity, Phishing, Email Hacks, Denial-of-service(DoS), Programming flaws, Spoofing attacks, Virus & Worms in Networks, Website Hacks, Leakage of Private information on blogs etc.

CONTRIBUTING VARIOUS SECTORS THROUGH CYBER CRIME SOLUTIONS

Being a Cyber Crime Investigation & Law Consultancy, Sytech Labs provides consultancy services to Cyber Law issues, helping Cyber Crime Victims and how to carry out Cyber Crime Investigations, etc. For this purpose, they have a panel of advocates/consultants specializing in Cyber Law matters and practicing at various levels over India.

He is Certified in

- Redhat Certified Security Specialist(**RHCSS**)
- Diploma in Microsoft Certified IT Professional (**MCITP**) Certification
- Diploma in Cisco Certified Network Professional (**CCNP**)
- Red Hat Linux(**RHCE**)
- CISCO Pix Firewall
- Certified Information Systems Security Professionals (**CISSP**).

Post Graguation In

- Post Graduate Diploma Cyber Law and Intellectual Property Law(**PGDCL&IPR**)
- Post Graduate Diploma Criminal Justice and Forensic Science(**PGDCJ&FS**)

WHY MILITARY MUST FOCUS ON CYBER SECURITY, MORE IMPORTANT THAN EVER BEFORE

The Prime Objective of the Indian Cyber Army is to establish a Professional Platform of understanding and thereby carrying out the development of cyber defence skills which in-turn will protect citizens, businesses, critical infrastructures of the state, and e-governance by establishing a collaborative platform for cybersecurity to provide a secure cyberspace to the society.

When we think of potential threats against commercial entities, the first thought is industry competitors wanting to steal company secrets and proprietary information. The military has secrets that, if leaked, could damage the security of the entire nation. So, their number one threat is potentially bad foreign actors wanting to learn military secrets, tactics, and plans.

National defence is central to protecting the territorial and political sovereignty of our republic. This defence is primarily provided by the military (Army, Navy and Air Force), with its soldier-and-weapon capability.

The effectiveness of military operations is finally based on the backup that the nation provides with its infrastructural, economic and political resources. Boots-on-the-ground in real-time combat situations cannot succeed without cyber-dependent operations and logistics. Thus there is a need for both offensive and defensive cyber capability and this is intimately linked with the cyber capability of the nation.

> *“THERE ARE REAL THREATS TO NATIONAL SECURITY FROM LOSS, LEAKAGE OR CORRUPTION OF DATA WHETHER DUE TO IGNORANCE, INADVERTENCE OR CYBERATTACK…”*

TRAINING INDIAN ARMY OFFICIALS ON CYBER SECURITY,CYBER CRIMES, THREAT MANAGEMENT SYSTEM AGAINST DEFENCE AND CYBER WARFARE TOOLS AT MILITARY COLLEGE OF ELECTRONICS & MECHANICAL ENGINEERING(MCEME),HYDERABAD

The effectiveness of military operations is finally based on the backup that the nation provides with its infrastructural, economic and political resources. Boots-on-the-ground in real-time combat-situations cannot succeed without cyber-dependent operations and logistics. Thus there is a need for both offensive and defensive cyber capability and this is intimately linked with the cyber capability of the nation.

The larger picture requires that data systems which include the bits and bytes which every civil and military computer stores, uses and processes, the enabling software, the basic hardware and the human resources which are the final users, are secure against loss, corruption, theft and infiltration. Thus, there are real threats to national security from loss, leakage or corruption of data whether due to ignorance, inadvertence or cyber attack. This calls for policy and coordination at the highest level, namely, the National Security Council (NSC).

Security of data at government or military levels is not unlike the privacy of personal data at the level of the individual. When the government stores and handles personal data of millions of its citizens in a national database, a cyber attack on such a database is an attack on national sovereignty.

THREATS TO INTER-CONNECTED DATABASES

In an age of exploding data, information and knowledge, both human and machine, cyber security is as much a necessity for personal privacy as it is for internal and external national security or for day-to-day economic activities and operation of social and economic infrastructure systems. Cyber security also constitutes the defensive part of modern warfare which is intimately connected with the blood-and-guts, on-the-ground military operations Thus, the threats to privacy and to national security from loss, leakage or corruption of data whether due to ignorance, inadvertence or cyber attack, need to be understood clearly.

TRAINING CUSTOMS AND COMMERCIAL TAX OFFICERS ON DATA EXTRACTION OF INFORMATION FROM DIGITAL DEVICES & CYBER SECURITY AT NATIONAL ACADEMY OF CUSTOMS, INDIRECT TAXES AND NARCOTICS(NACIN), VISAKHAPATNAM,ANDHRA PRADESH.

Tax practitioners have learned that they possess something that a new breed of criminals, namely cybercriminals, desire information.

The storage of taxpayer data in the Cloud and on open network systems provides a competitive advantage to tax practitioners to access.

Client information quickly and transmit data efficiently to the Internal Revenue Service and other state authorities on behalf of their clients.

CYBERCRIMINALS ADAPT TO A CHANGING ENVIRONMENT

The cybercriminals have evolved, adapted, and specialized in infiltrating electronic devices and exploiting the information stored therein. Additionally, the criminals have refined both who they target and how they pursue their ill-gotten gains.

As new defenses are erected that mitigate specific fraud schemes, cybercriminals develop new ruses or avenues that attack different participants in the tax return preparation process that may offer an easier path to success—the weakest link in the data security chain.

> “Preservation of evidence has become more complicated in recent years because of society’s increasing reliance upon electronic communications.”

WHY SECURITY AWARENESS TRAINING IS IMPORTANT TO EVERY ORGANIZATION

According to Verizon’s 2018 Data Breach Investigations Report, phishing or other forms of social engineering cause 93% of all data breaches. In order for phishing or social engineering attacks to be successful, the attacker needs a target to take the bait. Your employees often are the targets, aka the fish that bite. Employers must make employees aware of the risks associated with clicking on a link in a phishing email, downloading an attachment from an unknown sender or responding to requests for credential/login information or other data.

The only defense against such attacks is education — or in industry terms, "**Security Awareness Training**" — and falls squarely under the aegis of cybersecurity training, Because of the rapidly changing environment and long list of vulnerabilities, security awareness training also cannot involve a one-shot approch or a “ set it and forget it” program.

Preservation of evidence has became more complicated in recent years because of society’s increased reliance on electronic communication. Electronic versions of documents are more transient and subject to alteration. Ironically, they are also more transient and subject to alteration. Ironically, they are also more permanent, residing on the hard drives of many computer users for years. Versions of documents are frequently and routinely modified, overwritten, and perhaps deleted by computerized automatic deletion programs. Such events can become a serious issue in a dispute resolution process. The legal system has come up with a name for loss or destruction of evidence known as “spoliation.”

TRAINED VARIOUS STATE POLICE OFFICERS OF INDIA, JUDICIAL OFFICERS AND PUBLIC PROSECUTORS ON CYBER CRIME INVESTIGATION AND CYBER LAW AT CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Cyber crime has an expansive definition that includes any crime conducted via the Internet, network or digital device. Capturing digital evidence, such as that found on cellular phones, GPS devices, computers, tablets and network servers, is crucial to investigating and solving cyber crimes. Strong cyber crime investigative capabilities are also critical for solving traditional crime.

TWe describe the basic steps necessary when conducting the investigation, steps required to identify potential digital evidence, and how to work with different kinds of digital evidence (e.g. mobile devices, social media, IP addresses, etc).

TRAINING OFFICERS ON CYBER CRIME PROTOCOL

Chiefs should ensure that officers,investigators, and other relevant personnel receive regular training on handling cyber crimes.

CYBER CRIME POLICIES

Departments should develop policies and protocols for handling cyber crime investigations and what to do in case the agency is the victim of a hacking attack.

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD
Course on "Cyber Crime Investigation Course for Police Officers"
(14-01-2019 TO 18-01-2019)

Sitting (L to R): S/Sri:- Pushpendra Singh Baghel, Dy.SP(Chhattisgarh), Sandeep Mudalkar, Cyber Crime Investigator, Amrit Raj, IPS, DIG/Director, CDTI, R.S.Jaya Kumar, Vice Principal, Dr.Devaraja T.V, PI(Kar).

Standing 1(L to R): S/Sri:- Girish Ganpat Bane, PI(Mah), Miss.Kalpanaben J.Gouswami, PSI(Guj), Miss.Varsha Marotrao Kharsan, PSI(Mah), Ms.Aparajita Singh Rana, - - SI(Chhattisgarh), Ms.Sitabahen Mahadevbhai Rabari, PSI(Guj), Nilesh Kashinath Yashvantrao, PSI(Mah), E.Madan Mohan Raju, SI(TS), N.Madhu Sudhan Goud, SI(TS), Hrushikesh Meher, Inspr(Odisha).

Standing 2(L to R): S/Sri:- Jayprakash Rampal Nirmal, PSI(Mah), Sanjoy Ghosh, SI(WB), Ajay Kumar Sharma, SI(Del), Ashwini Kumar, Inspr(Bihar), Noone - - Venkateshwarlu, Inspr(TS), Yellaula Venkata Prasad, SI(TS), Mohammad Magdum Ali, SI(TS).

JURISDICTIONAL ISSUES

Cyber crime frequently crosses state and national borders. Chiefs should work with their federal law enforcement partners & local prosecutors to understand the jurisd- -ictional issues involved with cyber Crimes.

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD
Course on "Cyber Crime & Cyber Law Awareness Programme For Judicial Officers And Public Prosecutors"
(08-04-2019 To 10-04-2019)

Sitting (L to R): S/Sri:- Ajoy Prem Kumar Lam, Joint Director of Prosecution(AP), D.Kiran Kumar, Senior Civil Judge(TS), B.S. Jag Jeevan Kumar.Addl.District - -Judge(TS), Neelappa Ningappa Yalavatti, Senior Civil Judge(Kar), Amrit Raj, IPS, DIG, Director, CDTI, Sandeep Mudalkar, Cyber Crime - - Investigator, Ms.Kottu Sailaja, District & Sessions Judge(TS), Smt.D.Varoodhini, Senior Civil Judge(TS), R.S.Jaya Kumar, Vice Principal.

Standing 1(L to R): S/Sri:- Ankur Gupta, Asst.Public Prosecutor(Del), Smt.Ranjana Geeta, Asst.Public Prosecutor(AP), Smt.Suchitra Shailendra Narote, Asst.Public - - Prosecutor(Mah), Smt.I.Deepa Rani, Asst.Public Prosecutor(TS), Smt.V.Raja Rajeswari, Asst.Public Prosecutor(AP), Smt.Lingayat Sharayu - - Chandrashekhar, Asst.Public Prosecutor(Mah), Smt.Sandhya Chandrashekhar Kale, Asst.Public Prosecutor(Mah), Ms.M.Krishnaveni, - Public Prosecutor(Kar), Smt.Ashwini K.G, Sr.Asst.Public Prosecutor(Kar), Amardeep Ashok Chaware, Asst.Public Prosecutor - - Group-A(Mah).

Standing 2(L to R): S/Sri:- Talari Ramakrishna, Asst.Public Prosecutor(AP), Chander Kirti Negi, Asst.Public Prosecutor(Del), M.K.Shukla, Addl.Public Prosecutor(Del), Dharavath Raghu, Addl.Public Prosecutor Grade-II(TS), Prabhakar Jagannath Tarenge, Asst.Public Prosecutor(Mah), Nilesh Nivrutti - - Jadhao, Asst.Public Prosecutor(Mah).

ENSURING OFFICER/INVESTIGATORS UNDERSTAND DIGITAL EVIDENCE

Chiefs need to be aware of the wide variety of digital evidence their officers and investigators handle, and ensure that evidence is properly processed and stored.

> “ SOURCES OF DIGITAL EVIDENCE MAY NOT ALWAYS BE AS EASY TO RECOGNIZE AS A COMPUTER OR CELL PHONE FOUND AT THE SCENE. ”

“It’s important for all Police officers to understand cyber security as fully as possible. By doing so, they can develop their Knowledge in this increasingly important area, improving security in both their professional and personal lives.”

When conducting a cybercrime investigation, normal investigative methods are still important. Asking who, what, where, when, why and how questions is still important.

Pharmaceutical, Education & Tourism. domestic and foreign markets.

DIGITAL EVIDENCE

Digital evidence has become a ubiquitous part of criminal investigations with a presence that extends well beyond computer-specific crime. Frequent contact with digital devices in every facet of life produces so called 'digital exhaust' that can yield important clues regarding associations, location, and intent of both victims and suspects.

Sources of digital evidence may not always be as easy to recognize as a computer or cell phone found at the scene. Automobile navigation systems, video game consoles and other networked devices can also contain extremely important data. Similarly, online user accounts without any physical connection to a crime scene can yield important information about offline activities. Recognizing and preserving digital evidence is only one intersection with the lifecycle of a criminal investigation. Technical skills and infrastructure must be planned for in advance in order to field robust capabilities that can respond to investigative needs in a timely fashion. Coordination with other elements of the criminal justice system such as prosecutors, defense attorneys and judges are also crucial for employing digital evidence towards a successful prosecution.

RECOVERING DIGITAL EVIDENCE (DIGITAL FORENSICS)

Recovering and analyzing data and material obtained from electronic devices and cloud-based services, also known as digital forensics, can provide significant leads and digital evidence. While digital forensic analysts are responsible for conducting in-depth investigations of devices, first responders also play an important role in ensuring that any devices, and their content, are properly recovered and preserved.

CONDUCTING HANDS ON CYBER CRIME INVESTIGATION, DATA PRESERVING,COLLECTION OF DIGITAL EVIDENCE TO VARIOUS STATE POLICE OF INDIA AT POLICE STATE HEAD QUARTERS

LAW ENFORCEMENT OFFICERS TRAINED TO TACKLE CYBERCRIME

As technologies become ever more sophisticated, so too do the modus operandi of criminals, who are increasingly using information and communication technologies to carry out such illegal activities as fraud, online child sexual exploitation and abuse and phishing, to name only a few.

Cybercrime, also known as computer crime, e-crime, hi-tech crime or electronic crime, generally refers to any criminal activity in which a computer or network is the source, tool, target or place of a crime. Such crimes may be divided broadly into two categories: the first covers crimes that target computer networks or devices directly, while the second refers to those facilitated by computer networks or devices, the primary target of which is independent of the computer network or device.

> ***" Digital evidence preservation and maintenance should, at a minimum, follow agency standards and protocols. "***

Success Achievement Recognition

> “Without continual growth and progress, such words as improvement, achievement, and success have no meaning. Happiness does not come from doing easy work but from the afterglow of satisfaction that comes after the achievement of a difficult task that demanded our best.”

FOSTERING CYBERSECURITY THROUGH TRAINING THE JUDICIARY ON DIGITAL AND CYBER ISSUES

State court systems have an extraordinary responsibilityas the public guardians of sensitive digital data assets.Fortunately, the judicial branch is up to the challenge. Thebest administration of justice has long required the use of modern management techniques in daily court operations. Safeguarding confidential court recordsremains essential to protecting the rights and liberties of individuals and organizations.

To harness the resourcesnecessary to protect the public's data, the threats posedby cyberattacks must be met with increased internalcoordination and collaboration across branches. Through this process, courts can establish a data-governanceframework that protects the privacy of all involved in thejudicial process.

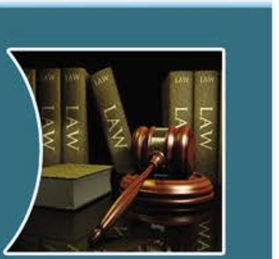
Court systems are guardians of sensitive data for individuals and organizations. But they cannot fulfill this responsibility alone.

CYBERSECURITY: PROTECTING COURT DATA ASSETS

This information is shielded from public view to protect the privacy of litigants, children, witnesses, judges, and employees. Courts are entrusted with these records, and consequently face varying degrees of liability if they fail to keep them secure. Many are negatively impacted by a cyberattack on a court: litigants, witnesses, victims, judges, lawyers, court staff, the organization itself, and the public as a whole.

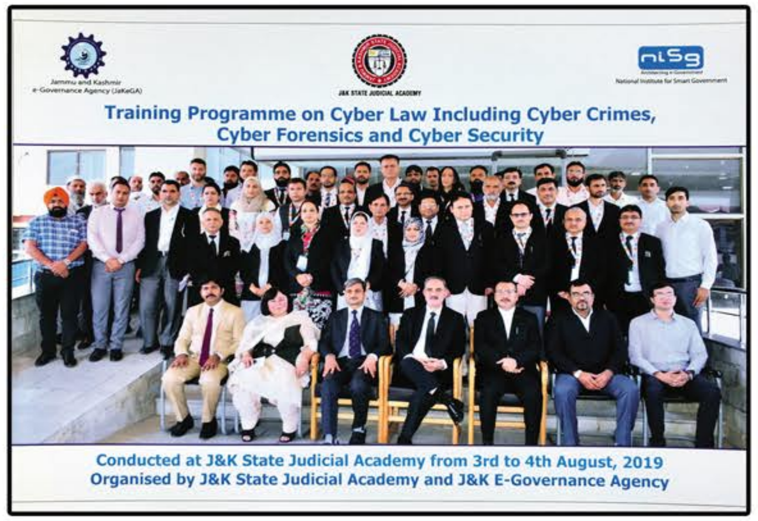
In addition to data-asset threats, shutting down court systems because of a cyberattack can have massive operational impact on normal court business. In these instances, courts must be able to hold time-sensitive and constitutionally mandated hearings, as well as issue warrants and orders. information, provides great value to the court community

TWO-DAY TRAINING FOR JUDICIAL OFFICERS, INVESTIGATORS, PROSECUTORS, LAW OFFICERS AND OFFICERS FROM ANTI CORRUPTION BUREAU ON CYBER-LAWS INCLUDING CYBER-CRIMES, CYBER-FORENSICS, CYBER LAW, CYBER-SECURITY ORGANISED BY NATIONAL INSTITUTE OF SMART GOVERNANCE(NISG), GOVT OF INDIA AT JUDICIAL ACADEMY, SRINAGAR IN STATE OF JAMMU AND KASHMIR.



The promulgation of laws relating to cybersecurity has enjoyed prominence at an international level for some years now, on account of the number, frequency, and impact of incidents recorded worldwide. Various initiatives regard legislation in this area as a fundamental factor that improves a country's maturity.

> *"Most cyber security laws are national in scope whereas the internet is not limited to national political or geographical boundaries, being borderless and International..."*


Training Programme on Cyber Law Including Cyber Crimes, Cyber Forensics and Cyber Security
Conducted at J&K State Judicial Academy from 3rd to 4th August, 2019
Organised by J&K State Judicial Academy and J&K E-Governance Agency

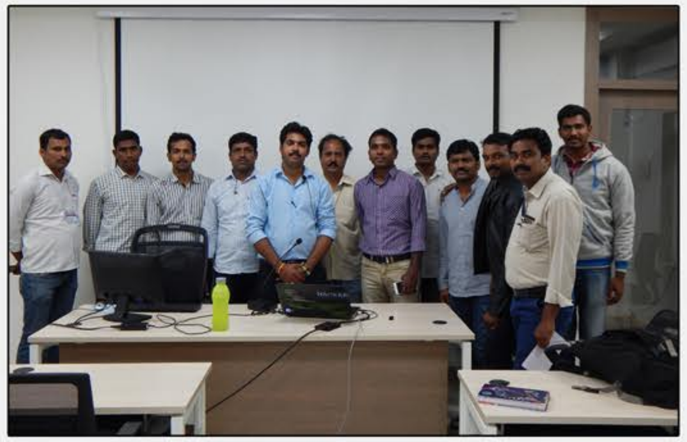
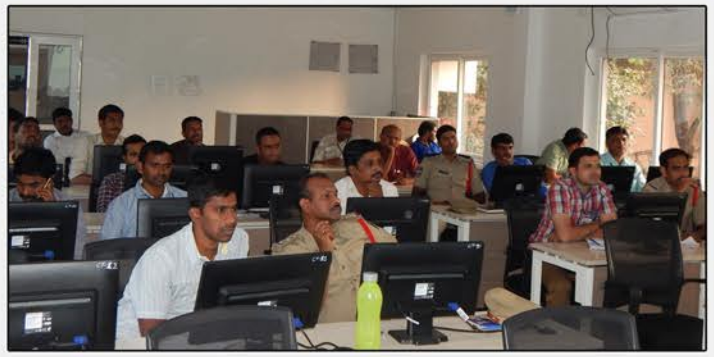
THREATS TO INTER-CONNECTED DATABASES

In an age of exploding data, information and knowledge, both human and machine, cyber security is as much a necessity for personal privacy as it is for internal and external national security or for day-to-day economic activities and operation of social and economic infrastructure systems. Cyber security also constitutes the defensive part of modern warfare which is intimately connected with the blood-and-guts, on-the-ground militar.

Cyber Security and its Best Practices at MCRHRDI(Govt of Telangana)& APHRDI(Govt of AP)

Dr.MCR HUMAN RESOURCE DEVELOPMENT INSTITUTE OF TELANGANA
TRAINING PROGRAMME ON
"NETWORKING & SECURITY"
FROM 02nd JULY TO 04th JULY 2018

Training on Cyber Crime Investigation to Hyderabad Cyber Cell,Telangana Police.

Cyber Security Tranning for Collectorates in association with Telangana Academy for Skill and Knowledge

Digital India Programs

MOU's with Various Organisations

CYBER SECURITY: CORPORATE TRAINING

WHY

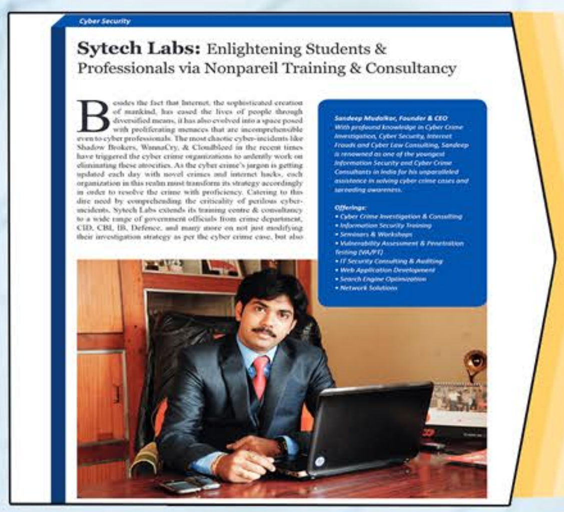
"Every organization is responsible for ensuring Cyber Security. The ability to protect its information systems from impairment or even theft is essential to success. Implementing effective Security measures will not only offer liability protection; it will also increase efficiency and productivity.

WE

"With our Cyber Security trainings your participants will understand the different types of malware and security breaches. Develop effective revention methods which will increase overall security. They will also understand the basic concepts associated with Cyber Security and what a company needs to stay secure.

"Cyber vulnerability is not only from critical hardware; sub-critical hardware is also vulnerable when purchased from international vendors…"

Into Media



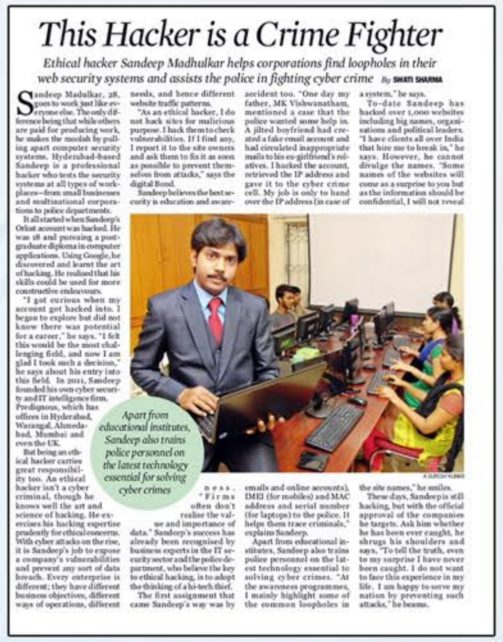
Cyber Security

Sytech Labs: Enlightening Students & Professionals via Nonpareil Training & Consultancy

Besides the fact that Internet, the sophisticated creation of mankind, has eased the lives of people through diversified means, it has also evolved into a space posed with proliferating menaces that are incomprehensible even to cyber professionals. The most chaotic cyber-incidents like Shadow Brokers, WannaCry, & Cloudbleed in the recent times have triggered the cyber crime organizations to ardently work on eliminating these atrocities. As the cyber crime's jargon is getting updated each day with novel crimes and internet hacks, each organization in this realm must transform its strategy accordingly in order to resolve the crime with proficiency. Catering to this dire need by comprehending the criticality of perilous cyber-incidents, Sytech Labs extends its training centre & consultancy to a wide range of government officials from crime department, CID, CBI, IB, Defence, and many more on not just modifying their investigation strategy as per the cyber crime case, but also

Sandeep Mudalkar, Founder & CEO
With profound knowledge in Cyber Crime Investigation, Cyber Security, Internet Frauds and Cyber Law Consulting, Sandeep is renowned as one of the youngest Information Security and Cyber Crime Consultants in India for his unparalleled assistance in solving cyber crime cases and spreading awareness.

Offerings:
- Cyber Crime Investigation & Consulting
- Information Security Training
- Seminars & Workshops
- Vulnerability Assessment & Penetration Testing (VA/PT)
- IT Security Consulting & Auditing
- Web Application Development
- Search Engine Optimization
- Network Solutions



This Hacker is a Crime Fighter

Ethical hacker Sandeep Madhulkar helps corporations find loopholes in their web security systems and assists the police in fighting cyber crime By SWATI SHARMA

Sandeep Madulkar, 28, goes to work just like everyone else. The only difference being that while others are paid for producing work, he makes the moolah by pulling apart computer security systems. Hyderabad-based Sandeep is a professional hacker who tests the security systems at all types of workplaces—from small businesses and multinational corporations to police departments.

It all started when Sandeep's Orkut account was hacked. He was 18 and pursuing a postgraduate diploma in computer applications. Using Google, he discovered and learnt the art of hacking. He realised that his skills could be used for more constructive endeavours.

"I got curious when my account got hacked into. I began to explore but did not know there was potential for a career," he says. "I felt this would be the most challenging field, and now I am glad I took such a decision," he says about his entry into this field. In 2011, Sandeep founded his own cyber security and IT intelligence firm, Prediqnous, which has offices in Hyderabad, Warangal, Ahmedabad, Mumbai and even the UK.

But being an ethical hacker carries great responsibility too. An ethical hacker isn't a cyber criminal, though he knows well the art and science of hacking. He exercises his hacking expertise prudently for ethical concerns. With cyber attacks on the rise, it is Sandeep's job to expose a company's vulnerabilities and prevent any sort of data breach. Every enterprise is different; they have different business objectives, different ways of operations, different needs, and hence different website traffic patterns.

"As an ethical hacker, I do not hack sites for malicious purpose. I hack them to check vulnerabilities. If I find any, I report it to the site owners and ask them to fix it as soon as possible to prevent themselves from attacks," says the digital Bond.

Sandeep believes the best security is education and awareness. "Firms often don't realise the value and importance of data." Sandeep's success has already been recognised by business experts in the IT security sector and the police department, who believe the key to ethical hacking, is to adopt the thinking of a hi-tech thief.

The first assignment that came Sandeep's way was by accident too. "One day my father, MK Vishwanatham, mentioned a case that the police wanted some help in. A jilted boyfriend had created a fake email account and had circulated inappropriate mails to his ex-girlfriend's relatives. I hacked the account, retrieved the IP address and gave it to the cyber crime cell. My job is only to hand over the IP address (in case of emails and online accounts), IMEI (for mobiles) and MAC address and serial number (for laptops) to the police. It helps them trace criminals," explains Sandeep.

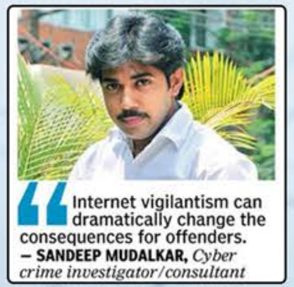
Apart from educational institutes, Sandeep also trains police personnel on the latest technology essential to solving cyber crimes. "At the awareness programmes, I mainly highlight some of the common loopholes in a system," he says.

To-date Sandeep has hacked over 1,000 websites including big names, organisations and political leaders. "I have clients all over India that hire me to break in," he says. However, he cannot divulge the names. "Some names of the websites will come as a surprise to you but as the information should be confidential, I will not reveal the site names," he smiles.

These days, Sandeep is still hacking, but with the official approval of the companies he targets. Ask him whether he has been ever caught, he shrugs his shoulders and says, "To tell the truth, even to my surprise I have never been caught. I do not want to face this experience in my life. I am happy to serve my nation by preventing such attacks," he beams.

Apart from educational institutes, Sandeep also trains police personnel on the latest technology essential for solving cyber crimes

A SURESH KUMAR



Internet vigilantism can dramatically change the consequences for offenders.
— SANDEEP MUDALKAR, *Cyber crime investigator/consultant*

మచ్చిక చేసుకొని.. ముంచేస్తారు..

[illegible]

CYBER SECURITY CONSULTANTS 201

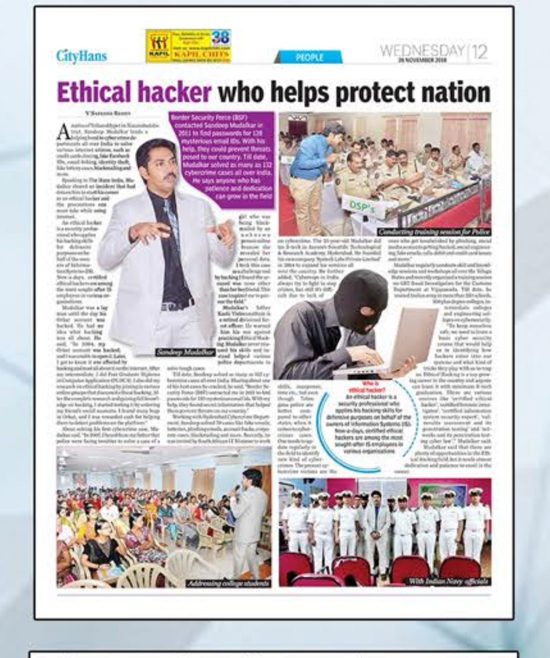
Sytech Labs:
Prioritizing Data Security in the Digital Age

[illegible]

The firm prides itself for the Corporate Security training seminars & workshops it conducts to enhance the knowledge base around Cyber security

సైబర్ నేరాల సమర సైనికుడు!

[illegible]



CityHans PEOPLE WEDNESDAY | 12 28 NOVEMBER 2018

Ethical hacker who helps protect nation

[illegible]

Border Security Force (BSF) contacted Sandeep Mudalkar in 2011 to find passwords for 120 mysterious email IDs. With his help, they could prevent threats posed to our country. Till date, Mudalkar solved as many as 132 cybercrime cases all over India. He says anyone who has patience and dedication can grow in the field

Sandeep Mudalkar

Conducting training session for Police

Who is ethical hacker?
An ethical hacker is a security professional who applies his hacking skills for defensive purposes on behalf of the owners of information Systems (IS). Now-a-days, certified ethical hackers are among the most sought-after IS employees in various organisations

Addressing college students

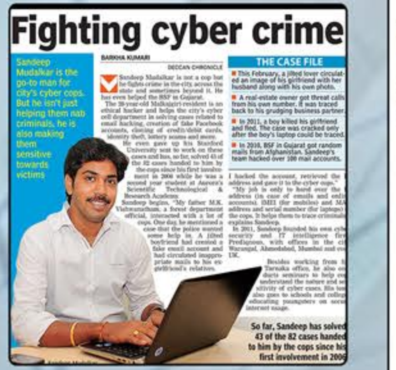
With Indian Navy officials

మాట్లాడుతున్న కలెక్టర్ సురేంద్రమోహన్

సాంకేతిక పరిజ్ఞానంపై అవగాహన పెంచుకోవాలి

[illegible]

ఆంధ్రజ్యోతి Sat, 15 July 2017



Fighting cyber crime

BARKHA KUMARI
DECCAN CHRONICLE

Sandeep Mudalkar is the go-to man for city's cyber cops. But he isn't just helping them nab criminals, he is also making them sensitive towards victims

Sandeep Mudalkar is not a cop but he fights crime in the city, across the state and sometimes beyond it. He has even helped the BSF in Gujarat.

The 28-year-old Malkajgiri-resident is an ethical hacker and helps the city's cyber cell department in solving cases related to email hacking, creation of fake Facebook accounts, cloning of credit/debit cards, identity theft, lottery scams and more.

He even gave up his Stanford University seat to work on these cases and has, so far, solved 43 of the 82 cases handed to him by the cops since his first involvement in 2006 while he was a second year student at Aurora's Scientific Technological & Research Academy.

Sandeep begins, "My father M.K. Vishwanatham, a forest department official, interacted with a lot of cops. One day, he mentioned a case that the police wanted some help in. A jilted boyfriend had created a fake email account and had circulated inappropriate mails to his ex-girlfriend's relatives. I hacked the account, retrieved the IP address and gave it to the cyber cops."

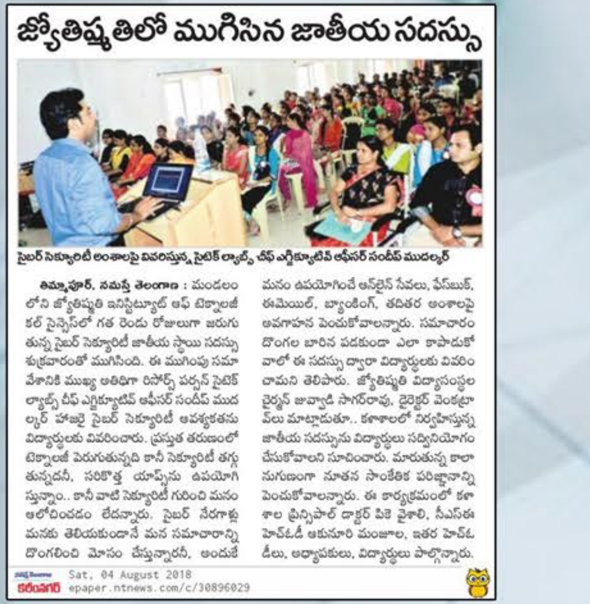
"My job is only to hand over the IP address (in case of emails and online accounts), IMEI (for mobiles) and MAC address and serial number (for laptops) to the cops. It helps them to trace criminals," explains Sandeep.

In 2011, Sandeep founded his own cyber security and IT intelligence firm Prediqnous, with offices in the city, Warangal, Ahmedabad, Mumbai and even UK.

Besides working from his Tarnaka office, he also conducts seminars to help cops understand the nature and sensitivity of cyber cases. His team also goes to schools and colleges educating youngsters on secure internet usage.

THE CASE FILE
- This February, a jilted lover circulated an image of his girlfriend with her husband along with his own photo.
- A real-estate owner got threat calls from his own number. It was traced back to his grudging business partner.
- In 2011, a boy killed his girlfriend and fled. The case was cracked only after the boy's laptop could be traced.
- In 2010, BSF in Gujarat got random mails from Afghanistan. Sandeep's team hacked over 100 mail accounts.

So far, Sandeep has solved 43 of the 82 cases handed to him by the cops since his first involvement in 2006



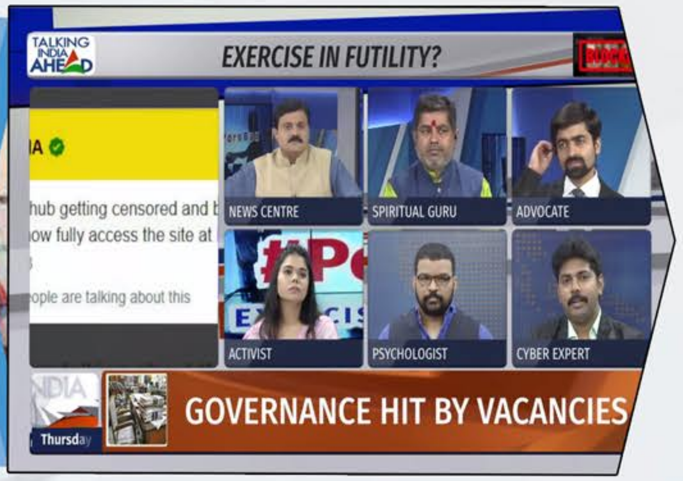
జ్యోతిష్మతిలో ముగిసిన జాతీయ సదస్సు

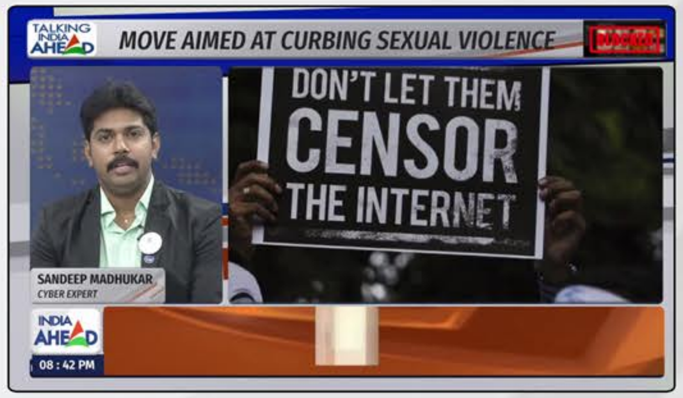
సైబర్ సెక్యూరిటీ అంశాలపై వివరిస్తున్న సైటెక్ ల్యాబ్స్ చీఫ్ ఎగ్జిక్యూటివ్ ఆఫీసర్ సందీప్ ముదల్కర్

తిమ్మాపూర్, నమస్తే తెలంగాణ : మండలంలోని జ్యోతిష్మతి ఇనిస్టిట్యూట్ ఆఫ్ టెక్నాలజీకల్ సైన్సెస్‌లో గత రెండు రోజులుగా జరుగుతున్న సైబర్ సెక్యూరిటీ జాతీయ స్థాయి సదస్సు శుక్రవారంతో ముగిసింది. ఈ ముగింపు సమావేశానికి ముఖ్య అతిథిగా రిసోర్స్ పర్సన్ సైటెక్ ల్యాబ్స్ చీఫ్ ఎగ్జిక్యూటివ్ ఆఫీసర్ సందీప్ ముదల్కర్ హాజరై సైబర్ సెక్యూరిటీ ఆవశ్యకతను విద్యార్థులకు వివరించారు. ప్రస్తుత తరుణంలో టెక్నాలజీ పెరుగుతున్నది కానీ సెక్యూరిటీ తగ్గుతున్నదనీ, సరికొత్త యాప్స్‌ను ఉపయోగిస్తున్నాం.. కానీ వాటి సెక్యూరిటీ గురించి మనం ఆలోచించడం లేదన్నారు. సైబర్ నేరగాళ్లు మనకు తెలియకుండానే మన సమాచారాన్ని దొంగలించి మోసం చేస్తున్నారనీ, అందుకే మనం ఉపయోగించే ఆన్‌లైన్ సేవలు, ఫేస్‌బుక్, ఈమెయిల్, బ్యాంకింగ్, తదితర అంశాలపై అవగాహన పెంచుకోవాలన్నారు. సమాచారం దొంగల బారిన పడకుండా ఎలా కాపాడుకోవాలో ఈ సదస్సు ద్వారా విద్యార్థులకు వివరించామని తెలిపారు. జ్యోతిష్మతి విద్యాసంస్థల చైర్మన్ జువ్వాడి సాగర్‌రావు, డైరెక్టర్ వెంకట్రావ్‌లు మాట్లాడుతూ.. కళాశాలలో నిర్వహిస్తున్న జాతీయ సదస్సును విద్యార్థులు సద్వినియోగం చేసుకోవాలని సూచించారు. మారుతున్న కాలానుగుణంగా నూతన సాంకేతిక పరిజ్ఞానాన్ని పెంచుకోవాలన్నారు. ఈ కార్యక్రమంలో కళాశాల ప్రిన్సిపాల్ డాక్టర్ పికె వైశాలి, సీఎస్‌ఈ హెచ్‌ఓడీ ఆకునూరి మంజుల, ఇతర హెచ్‌ఓడీలు, అధ్యాపకులు, విద్యార్థులు పాల్గొన్నారు.

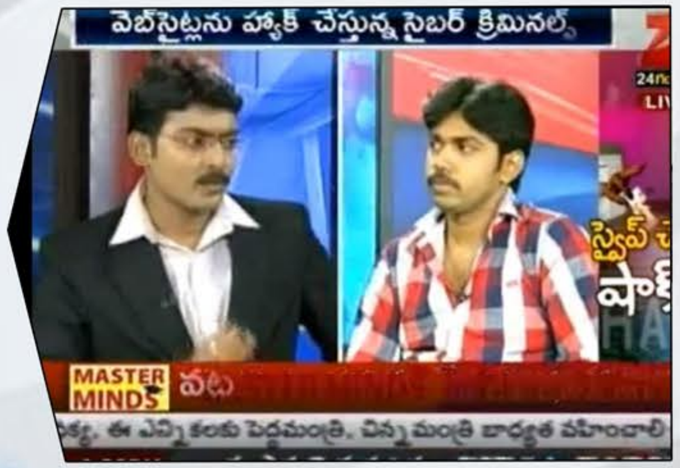
నమస్తే తెలంగాణ కరీంనగర్ Sat, 04 August 2018 epaper.ntnews.com/c/30896029

Eletronic Media

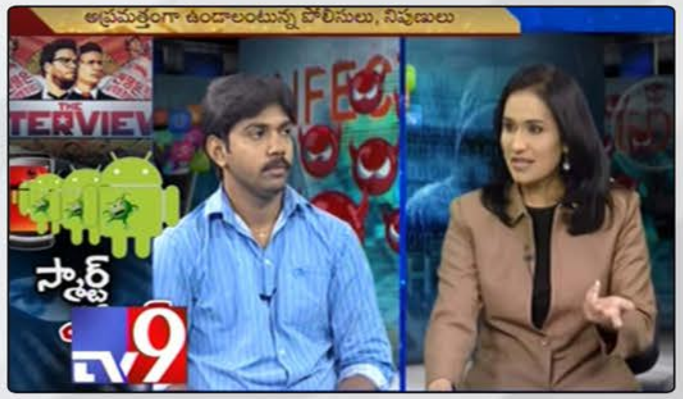


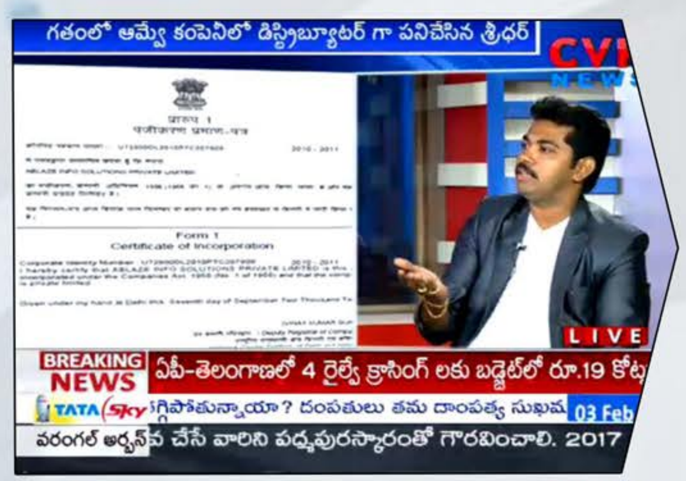


TALKING INDIA AHEAD
MOVE AIMED AT CURBING SEXUAL VIOLENCE
DON'T LET THEM CENSOR THE INTERNET
SANDEEP MADHUKAR
CYBER EXPERT
INDIA AHEAD
08 : 42 PM

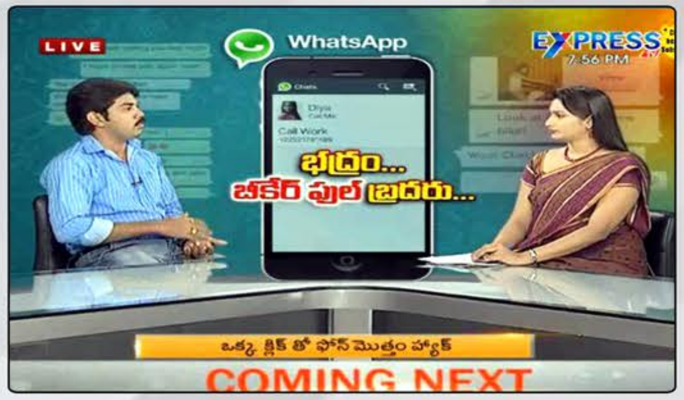


వెబ్‌సైట్లను హ్యాక్ చేస్తున్న సైబర్ క్రిమినల్స్
MASTER MINDS
స్టైఫ్ షాక్
కి, ఈ ఎన్నికలకు పెద్దమంత్రి, చిన్న మంత్రి బాధ్యత వహించాలి

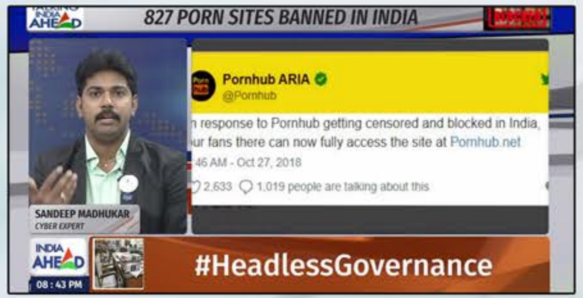




గతంలో ఆమ్వే కంపెనీలో డిస్ట్రిబ్యూటర్ గా పనిచేసిన శ్రీధర్
CVR NEWS
LIVE
BREAKING NEWS
ఏపీ-తెలంగాణలో 4 రైల్వే క్రాసింగ్ లకు బడ్జెట్‌లో రూ.19 కోట్ల
TATA Sky
గ్గిపోతున్నాయా? దంపతులు తమ దాంపత్య సుఖమ
03 Feb
వరంగల్ అర్బన్ సే చేసే వారిని పద్మపురస్కారంతో గౌరవించాలి. 2017



LIVE
WhatsApp
EXPRESS 7:56 PM
భద్రం... బీకేర్ ఫుల్ బ్రదరు...
ఒక్క క్లిక్ తో ఫోన్ మొత్తం హ్యాక్
COMING NEXT

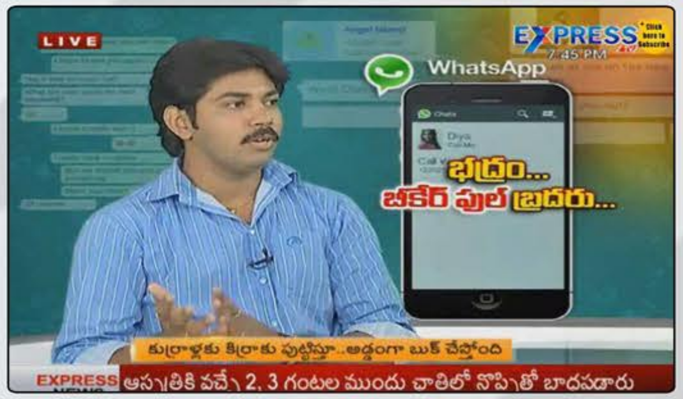


Pornhub ARIA
@Pornhub

In response to Pornhub getting censored and blocked in India, our fans there can now fully access the site at Pornhub.net

46 AM - Oct 27, 2018

2,633 1,019 people are talking about this



LIVE
EXPRESS 7:45 PM
WhatsApp
భద్రం... బీకేర్ ఫుల్ బ్రదరు...
కుర్రాళ్లకు కిలాడీ పుల్లలు...అడ్డంగా బుక్ చేస్తోంది
EXPRESS ఆసుపత్రికి వచ్చే 2, 3 గంటల ముందు చాటిలో నొప్పితో బాధపడుతూ

Sytech® Labs
Strengthening Cyber Security Private Limited

2018

2016

2017

2015

"Sytech labs presenting cyber security summits since 2014."

Awarness programmes on Cyber Crimes at Various Schools Across India

Workshops and Seminars at Variuous Engineering Colleges Across India

Sytech ®

Labs

Private Limited

Strengthening Cyber Security

CERTIFICATION

- Certified Ethical Hacker
- Certified Pentester
- Certified VA/PT & WA/PT
- Cyber Law
- Certified Forensic Investigator
- Certified Information Security Expert
- Certified Network & Its Penetration Testing
- Cyber Sense

OUR SERVICES

TRAININGs ON CYBER SECURITY
Welcome to Cyber Web..!! It's Interesting Word to Step-In..!!

CYBER CRIME INVESTIGATION & CONSULTING
If you're victim of cyber crime activity, we're here to catch them.

SOFTWARE DEVELOPMENT & SEO
Make your business global..!!

SEMINARS & WORKSHOPS
For College & School Students

CYBER LAWS CONSULTING
For whom who need legal Advice.

WEB APPLICATION PENTESTING
Protect your business

Address : Sri Sai Priya Appartment, #16-11-765, Door No: 203,Beside Sri Andal Nilayam American Tourister,
Near Cafe Coffee Day, Malakpet TV Tower, Moosarambagh, Hyderabad-500036. Phone : +91-8497953460.

Visit : www.sytechlabs.com | www.sandeepmudalkar.com | www.facebook.com/sytechlabs