

— CYBER DETECTIVE —

# CYBER CRIME INVESTIGATION

ONE STEP TOWARDS NATIONAL SECURITY

JAY HIND !



SPYRIOT SECURITY PVT. LTD.

# CYBER DETECTIVE TRAINING PROGRAM



## CYBER DETECTIVE

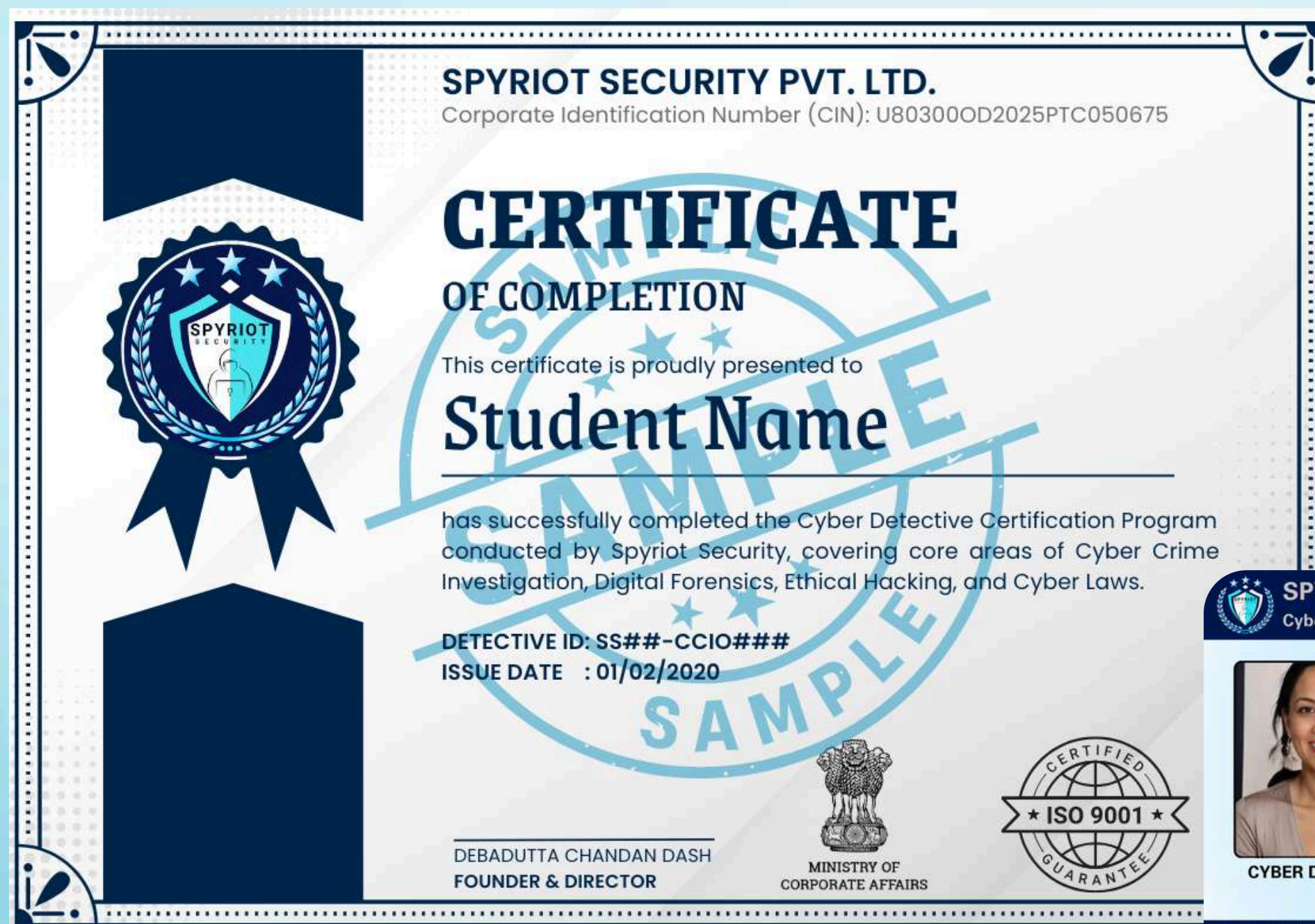


CRIME SCENE - DO NOT CROSS CRIME SCENE - DO NOT CROSS

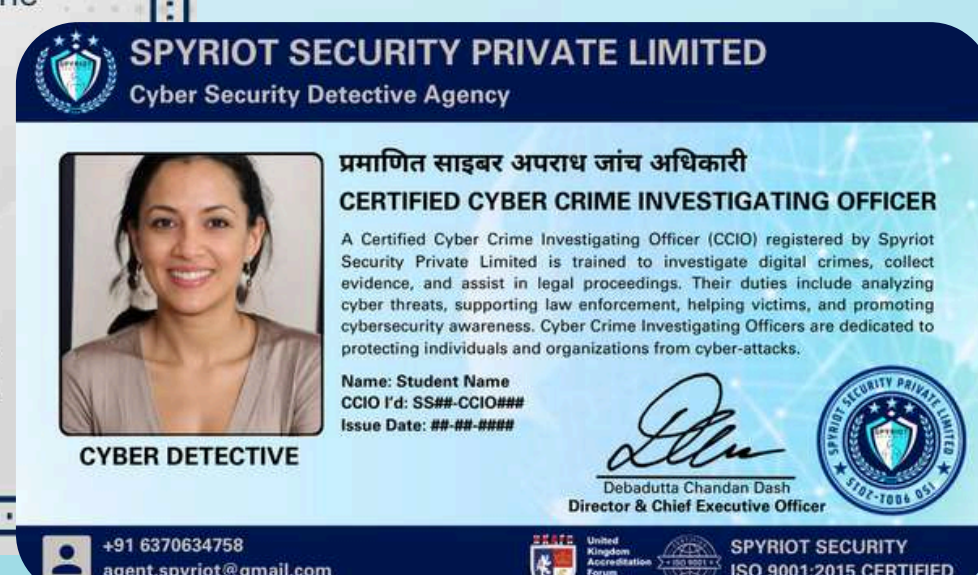
BEGINNER TO ADVANCED TRAINING

### Live Online Program Details:

Program	Cyber Crime Investigation
Duration	1 Month (Mon-Fri)
Course Fees	₹4,999 /- INR (Installment Available)
Training Mode	Live Online Classes
Class Timing	Evening 07:00 PM
Language	Hindi, English



### ISO Certificate & I'd Card





# SYLLABUS



## Module 1: Detective Mindset & Psychology

- Learn professional investigation psychology and disciplined detective thinking.
- Develop sharp observation, attention to detail, and emotional control.
- Understand human behavior, micro-expressions, and body language.
- Learn to Stay calm, neutral, and always maintain complete confidentiality.
- Study real-life case behaviors to recognize criminal patterns.
- Build strong ethics, patience, and a true investigator's mindset.

## Module 2: Core Intelligence & Investigation Operations

- Learn ground-level investigation and evidence collection techniques.
- Practice securing and documenting crime scenes to prevent contamination.
- Perform real-time surveillance using covert tracking, disguise, and observation.
- Apply psychological profiling for interrogation and lie detection mastery.
- Handle witnesses, suspects, and public interactions professionally.
- Prepare professional investigation reports with legal accuracy.

## Module 3: Legal Protocols and Forensic Evidence Handling

- Understand key Indian laws, cyber laws, and privacy regulations in detail.
- Learn the proper chain of custody for all physical and digital evidence.
- Draft clear, accurate legal reports and case documents for court submission.
- Collaborate effectively with law enforcement and intelligence agencies.
- Study detective licensing rules, registration process, and professional ethics.
- Master courtroom testimony and evidence presentation with confidence.

## Module 4: Cyber Crime & Digital Forensics Basics

- Understand cyber laws, global security policies, and major online crime types.
- Learn how to collect, preserve, and secure digital evidence effectively.
- Understand essential cyber forensic tools and investigation techniques.
- Perform incident response and reconstruct digital crime scenarios.
- Analyze real cyber-attack case studies and data breach investigations.
- Document forensic findings with professional reporting standards.

## Module 5: Network Investigation & IP Tracing Techniques

- Understand IP, DNS, and core network protocols exploited by cybercriminals.
- Perform packet capture and analysis using Wireshark and tcpdump tools.
- Detect suspicious network traffic and intrusion indicators effectively.
- Simulate phishing and DDoS attacks safely in a controlled lab environment.
- Use IP tracing and geolocation techniques to identify and track suspects.
- Create network forensics reports for cybercrime evidence.

## **Module 6: Undercover & Anonymous Operations**

- Create ethical covert identities, burner accounts, and controlled honeytraps.
- Use VPNs, encryption, and OPSEC methods for safe operations.
- Conduct anonymous cyber investigations on dark web platforms responsibly.
- Manage undercover communications securely and confidentially.
- Collect admissible digital evidence during undercover work with legal care.
- Plan safe mission exit strategies and thorough post-operation documentation.

## **Module 7: Spy Tools & Forensic Investigative Equipment**

- Learn practical use of spy cameras, GPS trackers, and covert audio recorders.
- Practice fingerprint collection, UV inspection, and other physical-evidence kits.
- Operate forensic imaging, hashing tools, and preserve data integrity correctly.
- Use OSINT platforms and digital monitoring apps for investigative lead generation.
- Maintain, secure, and troubleshoot investigative gadgets during field deployments.
- Prepare detailed evidence logs and technical documentation for lab submission.

## **Module 8: Social Engineering & Human Manipulation Techniques**

- Understand the psychology of deception and common manipulation tactics.
- Analyze phishing, vishing, pretexting, and baiting techniques with real examples.
- Identify emotional triggers attackers exploit to influence and deceive targets.
- Run controlled red-team social engineering simulations to test organizational defenses.
- Learn awareness and countermeasure techniques for prevention.
- Document and report social engineering case studies effectively.

## **Module 9: Specialized Cyber Crime Investigations**

- Investigate cases of online harassment, stalking, and digital blackmailing.
- Detect and deactivate fake social media profiles and deepfake scams.
- Investigate fake loan frauds, online scams, and digital financial crimes.
- Conduct phishing and fake job scam investigations with evidence collection.
- Analyze Android malware, malicious apps, and prevent sensitive data leaks.
- Investigate cyberbullying and online sexual harassment cases ethically and securely.

## **Module 10: Advanced Digital Forensics & System Analysis**

- Recover deleted files, logs, and artifacts from Windows and Linux systems.
- Analyze browser history, cache data, and saved credentials securely.
- Investigate network connections, user activity, and connected device logs.
- Extract metadata and enhance CCTV or image footage for clarity.
- Perform malware analysis and detect system compromise ethically.
- Prepare detailed forensic documentation and evidence recovery reports professionally.

## Module 11: Intelligence & Counter-Surveillance

- Build and manage informant networks to gather reliable human intelligence.
- Learn counter-surveillance tactics and anti-tracking techniques for safety.
- Use GPS, IMEI, and IP tracing tools to locate and trace suspects.
- Monitor suspects' digital footprints and real-world movements methodically.
- Plan and execute crisis or high-risk field operations with safety protocols.
- Coordinate intelligence sharing and joint operations with authorized agencies.

## Module 12: Career & Professional Branding

- Learn to establish and manage your own detective or investigation agency.
- Understand all legal registration, licensing, and compliance requirements.
- Build a strong professional brand and earn client trust effectively.
- Develop confident communication and impactful report presentation skills.
- Apply ethical marketing techniques to promote investigative services.
- Receive mentorship and career guidance for long-term professional success.

### Investigation Resources:

- PAN India leaked databases only for investigation purpose.(Free)
- Cyber detective practical study materials.(Free)
- Ethical hacking & cyber security study materials.(Free)
- Spy-Astra: Cybercrime investigation & hacking toolkit.(Paid)

**APPROVED BY: GOVERNMENT OF INDIA**



**United  
Kingdom  
Accreditation  
Forum  
Certification**



**MINISTRY OF  
CORPORATE AFFAIRS**



# CYBER DETECTIVE

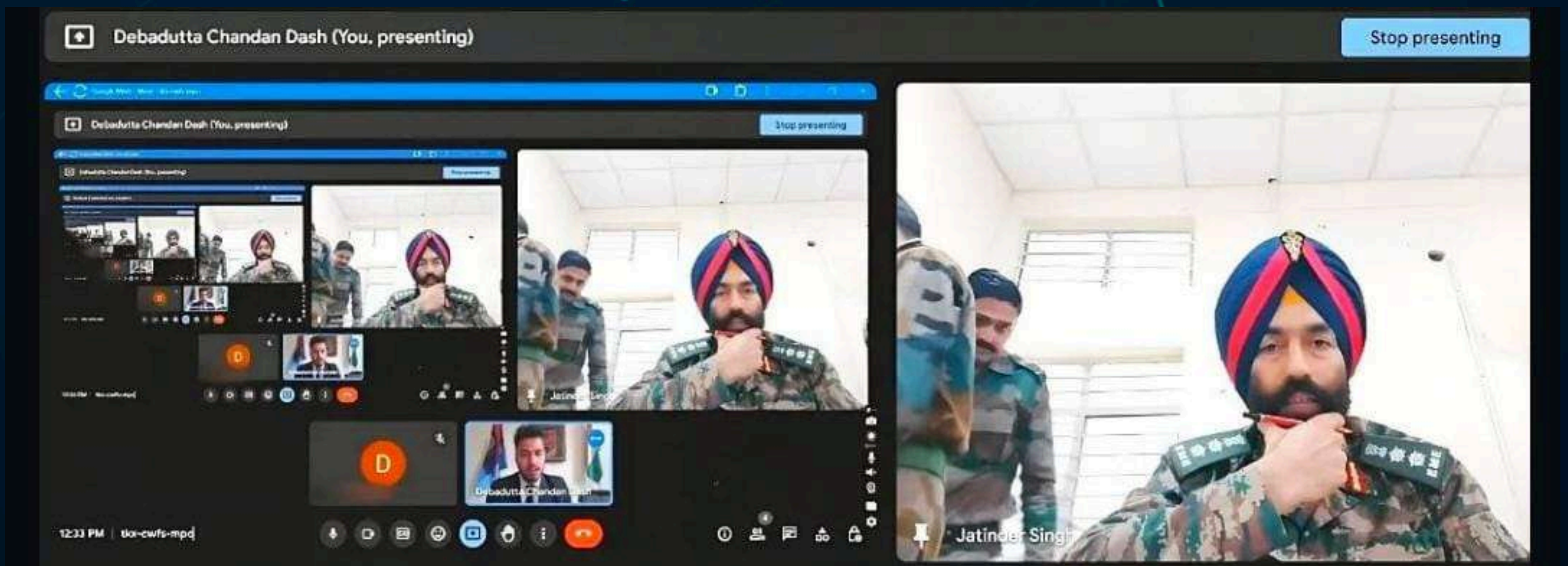
CYBER CRIME INVESTIGATOR | OSINT EXPERT

- Mastering Cyber Crime Investigations Through the Strategic Use of Open-Source Intelligence [OSINT].
- The Complete Guide for Professionals and Enthusiasts.



# Cybersecurity Awareness Program





# Empowering African Students Spyriot Security Pvt. Ltd. | India



# Cyber Security Training for Indian Army Spyriot Security Pvt. Ltd. | India



# Cybersecurity Training to Babzz ORG. | West Africa



# President of Nigerian Organization Ethical Hacking & Cyber Forensic Training



# Cyber Detective Program For German

SPYRIOT  
SECURITY



GERMANY





About  
Our Director:

# Director & CEO of Spyriot Security Pvt. Ltd.



## Debadutta Chandan Dash

A highly dedicated Indian Cyber Crime Investigator and the founder of Spyriot Security. Since 2020, Debadutta has been at the forefront of cybersecurity training and investigation, providing hands-on learning experiences through real-world projects and working closely with law enforcement agencies to solve complex cyber crime cases. He has trained students, corporate professionals, and government personnel. He also leads digital marketing and telecalling efforts to promote his training programs. His initiative includes an innovative e-learning platform tailored for rural students, delivering quality education through accessible online courses. Currently, Debadutta is expanding his reach across the globe. He has already taught professionals from Africa, Nigeria, Zimbabwe, Morocco, Afghanistan and Germany, reflecting his growing international presence. His vision is to empower the next generation of cyber defenders and promote a safer digital world for all.

## Our Mission

Our mission is to empower students with advanced knowledge and skills to combat cyber threats and safeguard Country's digital resources. Our training programs promote ethical hacking & cyber crime investigation practices and responsible use of cyber security techniques.

## Contact Us

For more information about Spyriot Security's cyber security training programs, please visit our website or contact us via email or phone.



Website

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



Email

[agent.spyriot@gmail.com](mailto:agent.spyriot@gmail.com)



Phone

[+91 6370634758](tel:+916370634758)