Marwadi University

CONTINUING EDUCATION PROGRAM (CEP)
On
Cyber Security, Forensics, Crimes and Laws

Marwadi University
Rajkot – Morbi Road, At & PO : Gauridad, Rajkot – 360 003, Gujarat. India.
+91 97277 24662 / 63 / 64 / 65
info@.marwadiuniversity.ac.in www.marwadiuniversity.ac.in

Program Objective

Cyber security is a collective effort of technologies, tools, policies and laws applicable to make cyberspace secure and safe. Information technology has enhanced the communication and has facilitated the growth of trade and commerce. The technology has fastened the e-commerce, e-Governance, net banking, mobile banking, online share trading and other commercial transactions. Due to increased number of cyber frauds, crimes, threats in real-world applications, organizations (both service provider and service consumers) require to adopt best practices for providing appropriate defense mechanism to protect their asset from malicious entities. Cyber criminals carry out online frauds and other criminal activities such as financial frauds, online defamation, data theft, obscenity, phishing, denial of service, violence, and so on. Online users should be conversant in judging whether they are falling in attacker's trap while using online services; enterprises should be comfortable in using third party services; application service providers/consumers must be familiar with ethical practices and legal aspects of data usage as well services, and aware of cyber laws applicable to cyberspace and consequences for violating cyber laws and unethical practices.

This program is offered by renowned security experts from academia and industry. The target audience comprising of Policy makers, Law makers, Implementers, Government officials, Bureaucrats, CEOs/CTOs/CFOs/CIO/CISOs of companies, IT professionals, IT managers, Banking professionals, Professionals of financial institutions, Faculty and Students. The significance of the program has added dimension in the current national focus and growth towards Smart Cities. All services covering sensors and sensor networks, ranging from home appliances, consumer electronics to border security, demand the awareness and understanding of implementation challenges of cyber security.

The program is a 22-hour (2 and ½ days) duration of intensive training with substantial emphasis on hands-on practices. The specially designed content of this program has been arrived upon after running shorter duration programs covering different modules of cyber security during last 5 years. Its content aims to provide with extensive training on various aspects of cyberspace security, challenges and defense mechanisms; digital forensics and detection of crimes; IT Act, cyber laws and legal aspects of IT/ITeS services. The course is equipped with cyber security fundamentals, essential cryptographic primitives, network security, web security, ethical hacking, perimeter security, system security, secure coding, access control, hardware security, vulnerability assessment, mobile security, cloud security, social network security and privacy, digital forensics, multimedia security, incident response, security risk management, ethical and legal aspects of digital data/service, cyber crimes and an intensive discussion on cyber laws with emphasis on Indian IT Act. The course modules emphasize adequate practical illustrations, case studies and hands-on sessions.

After going through this program, participants should be able to:

- Learn essential concepts in cyber security, security properties, threats and vulnerabilities in system and network security.
- Impart knowledge in web security, mobile security and defense mechanisms.
- Understand security aspects of application domain of e-Governance, e-Business, e-Contracts, e-Banking, e-Trading, online gaming, etc.

- Understand ethical hacking, various practical attacks and countermeasures, incident response and risk assessment.
- Show skills on hands-on experience in system security, email security, network security, ethical hacking, and incident response/countermeasures.
- Understand digital forensics, Windows, Linux and Mac security, Mobile forensics.
- Be familiar with different classes of cybercrimes and consequences.
- Be familiar with security policy, procedures, standards and best practices.
- Be familiar with Information Security Management System and training of effective IT Risk management.
- Get awareness of how the microchips and ICs that are fuelling every nook and corner of our cyber world are vulnerable to tampering in foundries.
- Get awareness of image tampering as a new cyber threat.
- Be conversant with Computer Frauds, Digital Frauds, Cybercrimes and consequences.
- Get desired exposure of Indian IT Act, IP, and conversant with cyber laws and legal practices

Program Coverage

The coverage of the program will have the following THREE verticals, where each vertical includes various topics suitable in its respective domain and maps to other verticals while addressing and/or assessing cyber security and legal characteristics in cyber space.

Study Material

Specially compiled exclusive study materials will be provided along with links of open source tools.

Cyber Security (System, Network & Web Security) [9 Hours]	Digital Forensics, Frauds and Crimes [7.5 Hours]	Cybercrimes, Cyber Laws [5.5 Hours]
-Cyber Security Basics -E-commerce security -Email security threats & countermeasures -Enterprise security -Network security -Web security threats & countermeasures -Ethical hacking -Vulnerability Assessment and Penetration Testing -Malwares (Virus, Worms, Trojan) -Perimeter security: Firewall, IDS/IPS, backup and recovery -Reverse engineering -Various attacks scenarios and defense mechanisms including Distributed Denial of Service attacks.	-Data and Image Forensic -Data Recovery -Forensic Investigation -Kill Switch – Security Threat at Hardware Level -Malware Analysis -Digital Forensics with Open-source tools -Social Media Forensics -Multimedia Forensics -Remote monitoring of surveillance system -Mobile Phone Forensics -Timeline Analysis -Various tampering/frauds/attacks and defense mechanisms in standalone and distributed platforms.	-Cybercrimes and digital frauds -Basics of E-commerce and Computer Fraud Techniques -Privacy and Security aspects in emerging lifestyles, Social Media security. -Cyber laws and legal aspects of digital age -IT Risk management -Security policy, best practices -Disaster recovery planning -IPR, copyright and legal issues -Indian IT Act -Service providers and consumer liability under IT Act Various cases of cybercrimes, card frauds, data frauds, consumer complaints, consequences and courts verdict.

Each vertical will have adequate illustrations of case study, demonstration and hands-on practice.

Who Can Attend?

The program is open for professionals and practitioners like Faculty, IT professionals, Banking professionals, Policy makers, Law makers, Government officials, CEOs/CTOs/CFOs/CIO/CISOs of companies, System administrator, and Students in the areas of Computer Science, Information Technology, Cyber security, Cyber law, Cyber forensics, Business Administration and allied fields.

This course is meant for everyone who uses computers, mobiles and Internet. Prior knowledge of either law or technology is NOT mandatory.

Duration and Schedule of the Program

DAY 1 (14th July 2017)

Registration 10.00 hrs – 10.30 hrs

CEP Objectives, Plan and Schedule 10.30 hrs – 11.00 hrs

Cyber Security, E-commerce & Enterprise security

[Speaker: Manik Lal Das] 11.00 hrs – 13.00 hrs

- **Cyber security threats, vulnerabilities and attacks**
- **Encryption/Decryption basics and application scenarios**
- **Computer Security, Access Control basics**
- **Enterprise security**
- **E-commerce security (Certification, TLS)**
- **Case Studies**

Lunch Break: 13.00 hrs – 13.45 hrs

Cyber space challenges, Surveillance system, Hardware security

[Speaker: Anil Roy] 13.45 hrs – 15.45 hrs

- **Cyber space security challenges**
- **Internet of Things – cyber physical space**
- **Surveillance system, Data/Image Tampering**
- **Virus, worms, spywares, ransom wares**
- **Hardware/Device security**
- **Case Studies**

Tea Break 15.45 hrs – 16.00 hrs

Cyber Crimes & Laws

[Speaker: Manan Thakker] 16.00 hrs – 18.30 hrs

- **Cybercrime techniques**
- **Cyber Contraventions & Compensation under I.T. Act, 2000**
- **Corporate Legal Liability under I.T. Act, 2000**
- **Adjudication Process for Recovery of Losses under I.T. Act, 2000**
- **Case Studies and Case Laws**

DAY 2 (15th July 2017)

Cyber Crime & Cyber Laws

[Speaker: Manan Thakker] 09.00 hrs – 10.30 hrs

- **E-signature and E-governance legality under I.T. Act, 2000**
- **ISPs and Websites Legal Liability under I.T. Act, 2000**
- **Regulating Cyber Space: National and International contexts**
- **Case studies**

Image and Data Forensics

[Speaker: Nilay] 10.30 hrs – 13.00 hrs

- **Forensic Imaging, Storage Media Duplication (FTK Imager)**
- **Windows Forensics Artifacts (Nirsoft/SysInternals)**
- **Forensic Investigation of Image (Autopsy)**
- **Digital Evidence & Forensic Toolkit (DEFT)**
- **Data Recovery (TestDisk / PhotoRec)**
- **Case studies, hands-on practice, or demonstration**

Lunch Break: 13.00 hrs – 13.45 hrs

Cyber Security and Ethical Hacking-1

[Speaker: Archit Agarwal] 13.45 hrs – 18.30 hrs

- **Email Hacking & its security**
- **SQL injection, Cross-site scripting**
- **Social Media Hacking & its Security**
- **Web Hacking & its Security**
- **Perimeter security – Firewalls, Routers, Bridges, IDS/IPS**
- **Case study and demonstration**

Tea Break 16.45 hrs – 17.00 hrs

DAY 3 (16th July 2017)

Cyber Crime & Cyber Laws

[Speaker: Manan Thakker] 09.00 hrs – 10.30 hrs

- **Computer Fraud Techniques**
- **E–contract & Electronic Data Interchange**
- **Basics of ISO 27001**
- **Security policy, compliance, standards**
- **Basics of Disaster recovery planning, Business continuity planning**
- **Case studies**

Cyber Security and Ethical Hacking–2

[Speaker: Archit Agarwal] 10.30 hrs – 13.00 hrs

- **Mobile Hacking & its Security**
- **Wi–Fi Network Hacking & its Security**
- **Windows Hacking & its Security**
- **Software Hacking & Reverse Engineering**
- **Data storage, Data leakage – security and privacy implications**
- **Case study and demonstration**

Lunch Break: 13.00 hrs – 13.45 hrs

Cyber and Media Forensics

[Speaker: Nilay] 13.45 hrs – 17.00 hrs

- **Registry, NTUSER.DAT, USERCLASS.DAT Analysis (Regedit, FRAT, Scripts)**
- **RAM Forensics (Concepts & Artifacts Analysis)**
- **Smart Phone Forensics (AFLogical, ViaForensics, MobileEdit)**
- **Multimedia Forensics (JPEGSnoop/ImageHeader Analysis)**
- **Case studies, hands–on practice, or demonstration**

Tea Break 16.45 hrs – 17.00 hrs

Examination (MCQ Pattern)

17.00 hrs – 18.00 hrs