

Department of Computer Science and Application
Atal Bihari Vajpayee Vishwavidyalaya, Bilaspur (C.G.)



Scheme and Syllabus
of
Post Graduate Certificate
in
Cyber Security & Cyber Law
(w.e.f. Academic Session 2019-20)

Program Code: PGC-003

1. About the Course

The Post graduate Certificate in cyber security and cyber law is an introductory course on the basics of Cyber Security, dealing with the different security models, cyber-attacks, cyber scams and frauds, the investigation mechanisms and cyber law. Learning the secure operations and the best practices are essential to protect each one of us from becoming the victims of cybercrimes. Fundamental knowledge is very much required to understand the current status of cyber world and how an individual or an organization or the government can safe-guard from the dangers in the cyber world.

Internet has led to widespread and drastic changes in our lives. Due to its reach and coverage, more and more processes and activities in organizations large and small are shifting online. Banking and Communication sectors are just a couple of glaring examples of this development. However, the ease of use brought about by computers has brought with it a significant rise in malicious attacks on digital devices and software systems. With increased dependence on computers and Internet, organizations are constantly exposed to high levels of business, operational and strategic risks. Hence, it is a challenge for these organizations to protect their data and systems from unauthorized access. This foundation program is geared towards generating and enhancing awareness about cyber security challenges and the concepts of cyber security and cyber ethics among the stake holders to help them become responsible cyber citizens and participate safely and securely in the rapidly evolving information-age society. This course is in line with the directions of UGC to introduce an elementary course in cyber security at UG and PG level across all the Indian Universities/ Institutions. Thus, the course aims to address information gaps among people with respect to cyber security. On successful completion of the exam, the student shall be provided with a mark sheet to be issued by AtalBihari Vajpayee University.

Scope

The learners will gain the absolute knowledge in the basics of Cyber Security. The usage of on-line facilities and complete automation of systems challenge the digital communication through various threats and vulnerabilities. Knowing the essentials of safe operations in the digital world will definitely prepare the learners on the technicalities, best practices and strategies to be used in the digital era.

2. Program Learning Outcome

After completion of this program the students will, be able to:

- Understand the fundamental concepts in cyber security and distinguish among the attacks, threats and vulnerabilities.
- Classify and explain different types of security architectures and defense methods.
- Identify, differentiate and explains different cybercrimes and frauds.

—
—



Shriya

- Apply different cyber-crime investigations method and techniques for typical cases, study the cases with human psychological profiling and develop suitable processes forensic investigations.
- Review and apply many of the existing approaches followed in cyber-crime detection and evaluate the same.
- Appreciate and adopt the best practices in cyber security.
- Evaluate the computer network and information security needs of an organization.
- Assess cybersecurity risk management policies in order to adequately protect an organization's critical information and assets.
- Measure the performance of security systems within an enterprise-level information system.
- Troubleshoot, maintain and update an enterprise-level information security system.
- Implement continuous network monitoring and provide real-time security solutions.
- Formulate, update and communicate short- and long-term organizational cybersecurity strategies and policies.
- Identify some of the factors driving the need for network security
- identify and classify particular examples of attacks
- Define the terms vulnerability, threat and attack
- Identify physical points of vulnerability in simple networks
- Compare and contrast symmetric and asymmetric encryption systems and their vulnerability to attack, and explain the characteristics of hybrid systems.
- Identify and rectify the problems related to Cyber security and cyber crime.
- Perform investigation related to cyber crime.

3. Eligibility Criteria

Any graduate either studying in PG or not, Working professionals from Police or any other relevant departments where knowledge of Cyber Security and Cyber Crime are needed and applicable.

4. Fees structure

One-time tuition fees of Rs. 5000/- + Misc. Fee as applicable

5. Intake-30 Seats

6. **Duration** –6 Months (probably from August to January)

7. Scheme of Examination

S No.	Course Name	Marks		Credit
		MAX	MIN	
1	Theory: Cyber Security and Cyber Law	100	40	4
2	Practical Based On Theory	100	40	2
Total		200	80	6

Note: Minimum Pass marks 40%

~~_____~~ *Shriya*

8. Course Contents

Module 1: Introduction to compute: Characteristics of computer, Types of computer, H/W and S/W, Types of software ,Operating system and their types, Security features of Windows and Linux.

Module 2: Overview of computer network: Types of computer Network: LAN, MAN, WAN Overview of Internet, Benefits and drawbacks of internet, Configuring Internet in your PC.

Module 3:OSI and TCP/IP reference Model: Various protocols, application layers programs like FTP, telnet etc., IP address and its types, Client – server model, DHCP, DNS,WWW and web server.

Module 4: Cyber Security Basics: Security Principles, Introduction to Cyber Crimes, Classification of Cyber Crime, Reasons for Commission of Cyber Crimes.

Module 5: Cyber Attack and their classification: Cyber Stalking, Child Pornography, Forgery and Counterfeiting, Software Piracy and crime related to IPRs, Cyber Terrorism, Phishing, Computer Vandalism. Spamming , Different types of attack.

Module 6: Authentication: Department of Computer Science and Application Vulnerability Assessment, Intrusion Detection and Intrusion Prevention System,Authentication, User Authentication Methods, Bio-metric Authentication Methods.

Module7: Windows Security: Working with Windows Firewall in Windows, Firewall in Windows 7, Configuring Windows Firewall, Start & Use the Windows Firewall with Advanced Security, , Windows Firewall with Advanced Security Monitor, Password security, Antivirus security.

Module 8: Different securities: Web Security, E-mail Security, Cloud Security, IoT Security, Cyber Physical System Security, and Social Media Security.

Module 9: Safe Browsing: Tips for Buying Online, Tips for using Social Networking platforms safely, Posting personal details, Friends-Followers & Contacts, Status Updates, Sharing Online Content, Revealing Your Location, Sharing Videos & Photos, Instant Chats, Joining and creating Groups, Events and Communities.

Module 10: Smartphone Security: Guidelines, Purses, Wallets, Smartphones, Platforms and Operating Systems, Feature Phones, Branded and locked smartphones, General setup, Installing and updating applications.

Module 11: Virtual Currencies , Block Chain Technology, Security Auditing.



Module 12: Cyber Crime: Types, Data frauds, Analysis of Crimes, Human Behavior, Stylometry, Incident Handling.

Module 13: Digital Forensics: History, Challenges ,Branches, Investigation Methods, Reporting, Management of Evidence, Investigation Methods, Criminal Profiling, Cyber Trails.

Module 14: Cyber Law-Basics: Information Technology Act 2000-Amendments.

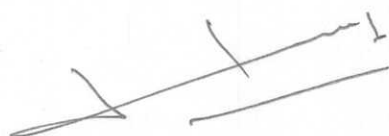
Module 15: Cyber law: Evidentiary value of E-mails/SMS, Cybercrimes and Offences dealt with IPC-RBI Act-IPR in India, Jurisdiction of Cyber Crime, Creating awareness and Healthy practices.

REFERENCES

1. Cyber criminology : Exploring Internet Crimes and Criminal Behavior by k. Jaishankar, CRC press.
2. Cryptography ,Network security and Cyber law by Bernard L. Menezes and Ravinder Kumar, Cinage learning
3. An unofficial guide to ethical hacking by ankit fadia , trinity publisher.
4. An ethical guide to hacking mobile phones by Ankit fadia, trinity publisher.
5. Computer Network Security and Cyber Ethics by Siva Ram Murthy,B.S. Manoj , McFarland and Company , INC
6. Data communication and Networking by B. Forouzan, TMH.
7. Cryptography and network security by William stalling, Pearson publication.

E- BOOKS LINK

1. https://heimdalsecurity.com/pdf/cyber_security_for_beginners_ebook.pdf
2. <http://larose.staff.ub.ac.id/files/2011/12/Cyber-Criminology-Exploring-Internet-Crimes-and-Criminal-Behavior.pdf>
3. <http://docshare04.docshare.tips/files/21900/219006870.pdf>
4. http://index-of.co.uk/Hackin_%20Beyond%20the%20Hacker.pdf
5. <http://www.uou.ac.in/sites/default/files/slm/FCS.pdf>



Shriya