

Part A Introduction			
Program: Degree	Class: B.A./B.Sc./B.Com./B.H.Sc./BCA	Year: III Year	Session: 2023-24
Subject: Foundation Course			
1.	Course Code	X3-FCBD1T	
2.	Course Title	Digital Awareness - Cyber Security	
3.	Course Type	Ability Enhancement Compulsory Course	
4.	Pre-requisite (if any)	Compulsory for all Third Year students	
5.	Course Learning outcomes (CLO)	<p>After completing the course, student will be able to :</p> <ul style="list-style-type: none"> ● Make optimum use of web browsers, search engines and Chatbots ● Creating e-mail account, sending, receiving and managing emails. ● Describe reporting procedure of phishing emails. ● Identify email phishing attack and preventive measures. ● Configure security settings in Mobile Wallets and UPIs. ● Practice safe, legal and ethical means of using Information Technology. ● Practice and use the various online financial and government services of day-to-day use. ● Understand the basic concepts related to E-Commerce and digital payments. ● Discuss cyber security aspects, RBI guidelines and preventive measures against digital payment frauds. ● Explore and learn the online available courses of his/her interest. ● Use the Digilocker and Academic Bank of Credit. ● Describe the concept of Cyber security and issues and challenges associated with it. . ● Explain the process of reporting cyber crime at Cyber crime Police Station/ at online platform. ● Appreciate various privacy and security concerns on online Social media. ● Guide through the reporting procedure of inappropriate content. ● Perform privacy and security settings for popular Social media platforms. 	
6.	Credit Value	2	
7.	Total Marks	Max. Marks: 50	Min. Marks:

Part B – Content of the Course		
	Total No. of Lectures 30 (01 hour per week)	
Unit	Topics	No. of Lectures
I	<p>Overview of Computer and Web-technology, Architecture of cyberspace, World wide web, Advent of internet, Internet infrastructure for data transfer and governance, Internet society.</p> <p>Use of Internet: Web browsers, search engines and Chatbots. Difference between Website & Portal, E-mail: Account opening, sending & receiving e-mails, managing Contacts & Folders.</p> <p>Computer Security: Issues & protection, firewall & antivirus, making secure online transactions. Internet safety and digital security. Ethical use of digital resources, Measures of Online Self Protection.</p> <p>Keywords: <i>Browser, Search Engine, Website, Virus, Security, Firewall, Cyber Ethics.</i></p>	05
II	<p>Digital Payments and e-Commerce:</p> <p>Internet Banking: National Electronic Fund Transfer (NEFT), Real Time Gross Settlement (RTGS), Immediate Payment Service (IMPS)</p> <p>Digital Financial Tools: Understanding OTP [One Time Password], QR [Quick Response] Code, UPI [Unified Payment Interface], AEPS [Aadhaar Enabled Payment System]; USSD [Unstructured Supplementary Service Data], Card [Credit / Debit], eWallet, PoS [Point of Sale]</p> <p>Definition of E-Commerce- Main components of E-Commerce, Elements of E-Commerce security, E-Commerce threats, E-Commerce security best practices, Online Bill Payment. Digital payments related common frauds and preventive measures. RBI guidelines and provisions of Payment Settlement Act, 2007.</p> <p>Keywords: <i>Internet Banking, Digital Financial Tools, eWallet, e-Commerce Security.</i></p>	07
III	<p>e-Governance Service-</p> <p>Overview of e-Governance Services like Railway Reservation, passport, eHospital; Accessing various e-Governance Services on Mobile Using “UMANG APP”. Exploring services and resources of Government of India Portal (https://www.mygov.in/).</p> <p>Digi-Locker: About digilocker, features and benefits of digilocker, Registering, accessing and getting various certificates and mark sheets on digilocker.</p> <p>Academic Bank of Credit (ABC): About ABC, features and benefits of ABC, Registering, accessing, getting and sharing academic credits.</p> <p>Exploring Online Learning resources: Online learning through SWAYAM Central, (https://swayam.gov.in/) and e-pathshala (https://epathshala.nic.in/).</p> <p>Keywords: <i>Internet Banking, NEFT, RTGS, IMPS, OTP, UPI, QR Code, AEPS, E-Governance, Umang.</i></p>	06

IV	Introduction to Cyber security- Regulation of cyberspace, Concept of cyber security, Issues and challenges of cyber security. Definition of cyber crimes and offences, Cyber crime targeting computers and mobiles, Cyber crime against women and children, Cyber bullying. Financial frauds, Social engineering attacks, Malware and Ransomware attacks, zero day and zero click attacks. Cyber criminals modus-operandi, Reporting of cyber crimes, Remedial and mitigation measures, Legal perspective of cyber crime, IT Act 2000 and its amendments, Organisations dealing with Cyber crime and Cyber security in India, Case studies. Keywords: Cyber Space, Cyber Security, Cyber Offences, Zero Click Attack, Zero Day Attack, Ransomware, Reporting Cyber Crimes, Cyber Crimes Case Studies.	05
V	Social Media Overview and Security- Introduction to Social Networks, Types of Social media, Social media platforms, Social media monitoring, Hashtag, Viral content, Social media marketing, Social media privacy, Challenges, opportunities and pitfalls in online social network, Security issues related to social media, Flagging and reporting of inappropriate content, Laws regarding posting of inappropriate content, Best practices for the use of Social media, Case studies. Keywords: Social Media Platforms, Hashtagging, Social Media Marketing, flagging of contents in social media.	06

Part C-Learning Resources

Text Books, Reference Books, Other resources

Suggested Readings:

- Praveen Kumar Shukla, Surya Prakash Tripathi, Ritendra Goel "Introduction to Information Security and Cyber Laws" Dreamtech Press.
- Vivek Sood, "Cyber law simplified", Tata McGrawHill, Education (India).
- T. Bradley "Essential Computer Security: Everyone's Guide to Email, Internet, and Wireless Security".
- Cyber Crime Impact in the New Millennium, by R. C Mishra , Auther Press. Edition 2010.
- Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd. (First Edition, 2011)
- Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform. (Pearson , 13th November, 2001)
- Electronic Commerce by Elias M. Awad, Prentice Hall of India Pvt Ltd.
- Cyber Laws: Intellectual Property & E-Commerce Security by Kumar K, Dominant Publishers.
- Network Security Bible, Eric Cole, Ronald Krutz, James W. Conley, 2nd Edition, Wiley India Pvt. Ltd.
- Fundamentals of Network Security by E. Maiwald, McGraw Hill

Reference Books:

- M. Stamp, "Information Security: Principles and Practice", Wiley.
- David J. Loundy, "Computer Crime, Information Warfare, And Economic Espionage", Carolina Academic Press.

Suggested equivalent online courses: e-reading:

- <http://egyankosh.ac.in/handle/123456789/9489>
- https://workspace.google.com/intl/en_in/training/
- <https://www.classcentral.com/course/openlearn-science-maths-technology-preparing-your-96104>
- <https://www.udemy.com/course/free-computer-literacy-101-course/>
- <https://www.mygov.in/>
- <https://epathshala.nic.in/>
- <https://www.digilocker.gov.in/>
- <https://www.abc.gov.in/>
- <https://swayam.gov.in/>

PART D: Assessment and Evaluation

Suggested Evaluation Methods:

Maximum Marks: 50

University Exam (UE): 50 Marks

External Assessment:	50 Objective type questions	50 Marks
University Exam (UE):		
Time : 01.00 Hours		

Any remarks/suggestions:

भाग अ - परिचय			
कार्यक्रम: उपाधि	कक्षा: बी.ए.एससी.बी./कॉम.बी./एससी.एच.बी./बी.सी.ए.	वर्ष: तृतीय	सत्र: 2023-24
विषय: आधार पाठ्यक्रम			
1	पाठ्यक्रम का कोड	X3-FCBD1T	
2	पाठ्यक्रम का शीर्षक	डिजिटल जागरूकता-साइबर सुरक्षा	
3	पाठ्यक्रम का प्रकार	योग्यता संवर्धन अनिवार्य पाठ्यक्रम	
4	पूर्वापेक्षा (Prerequisite) (यदि कोई हो)	तृतीय वर्ष के सभी विद्यार्थियों के लिए अनिवार्य	
5	पाठ्यक्रम अध्ययन की परिलब्धियां (कोर्स लर्निंग आउटकम) (CLO)	<p>इस पाठ्यक्रम के सफल समापन पर, विद्यार्थी निम्न में सक्षम होंगे:</p> <ul style="list-style-type: none"> ● वेब ब्राउज़र, सर्च इंजन और चैटबॉट्स का उपयोग । ● ई-मेल खाता बनाना, ईमेल भेजना, प्राप्त करना और प्रबंधन । ● फ़िशिंग ईमेल की रिपोर्टिंग की प्रक्रिया का वर्णन । ● ईमेल फ़िशिंग अटैक और निवारक उपायों की पहचान । ● मोबाइल वॉलेट और UPI में सुरक्षा सेटिंग्स कॉन्फ़िगर करना । ● सूचना प्रौद्योगिकी का उपयोग करने के सुरक्षित, कानूनी और नैतिक मानकों के साथ प्रयोग । ● दैनिक उपयोग की विभिन्न ऑनलाइन वित्तीय और सरकारी सेवाओं का उपयोग । ● ई-कॉमर्स व डिजिटल भुगतान संबंधी बुनियादी अवधारणाओं की समझ । ● साइबर सुरक्षा पहलुओं, आरबीआई के दिशानिर्देशों और डिजिटल भुगतान में धोखाधड़ी के निवारक उपाय । ● उसकी रुचि के ऑनलाइन उपलब्ध पाठ्यक्रमों को एक्सप्लोर करना । ● डिजिटल और अकादमिक बैंक ऑफ़ क्रेडिट का उपयोग । ● साइबर सुरक्षा की अवधारणा और इससे जुड़े मुद्दों और चुनौतियां । ● साइबर अपराध पुलिस स्टेशन/ऑनलाइन प्लेटफॉर्म पर साइबर अपराध की रिपोर्ट करने की प्रक्रिया । ● ऑनलाइन सोशल मीडिया पर विभिन्न गोपनीयता और सुरक्षा । ● अनुपयुक्त सामग्री की रिपोर्टिंग प्रक्रिया । ● लोकप्रिय सोशल मीडिया प्लेटफॉर्म के लिए गोपनीयता और सुरक्षा सेटिंग। 	
6	क्रेडिट मान	2	
7	कुल अंक	अधिकतम अंक: 50	न्यूनतम उत्तीर्ण अंक:

भाग ब- पाठ्यक्रम की विषयवस्तु		
कुल व्याख्यान संख्या- 30 (प्रति सप्ताह 01 घंटा)		
इकाई	विषय	व्याख्यान संख्या (1 घंटा/ व्याख्यान)
I	<p>कंप्यूटर और वेब-प्रौद्योगिकी का अवलोकन, साइबरस्पेस का आर्किटेक्चर, वर्ल्ड वाइड वेब, इंटरनेट का आगमन, डेटा ट्रांसफर और गवर्नेंस के लिए इंटरनेट इंफ्रास्ट्रक्चर, इंटरनेट समाज।</p> <p>इंटरनेट का उपयोग: वेब ब्राउज़र, सर्च इंजन और चैटबॉट्स। वेबसाइट और पोर्टल, ई-मेल के बीच अंतर, ई-मेल खाता खोलना, ई-मेल भेजना और प्राप्त करना, कॉन्टेक्ट्स और फ़ोल्डर का प्रबंधन।</p> <p>कंप्यूटर सुरक्षा: मुद्दे और सुरक्षा, फ़ायरवॉल और एंटीवायरस, सुरक्षित ऑनलाइन लेनदेन करना। इंटरनेट सुरक्षा और डिजिटल सुरक्षा। डिजिटल संसाधनों का नैतिक उपयोग, ऑनलाइन आत्म सुरक्षा के उपाय।</p> <p>Keywords: <i>Browser, Search Engine, Website, Virus, Security, Firewall, Cyber Ethics.</i></p>	05
II	<p>डिजिटल भुगतान और ई-कॉमर्स:</p> <p>इंटरनेट बैंकिंग: नेशनल इलेक्ट्रॉनिक फंड ट्रांसफर (एनईएफटी), रीयल टाइम ग्राँस सेटलमेंट (आरटीजीएस), तत्काल भुगतान सेवा (आईएमपीएस)</p> <p>डिजिटल वित्तीय उपकरण: ओटीपी [वन टाइम पासवर्ड], क्यूआर [क्विक रिस्पॉंस] कोड, यूपीआई [यूनिफाइड पेमेंट इंटरफेस], एईपीएस [आधार सक्षम भुगतान प्रणाली] को समझना; USSD [अनस्ट्रक्चर्ड सप्लीमेंट्री सर्विस डेटा], कार्ड [क्रेडिट/डेबिट], ई-वॉलेट, PoS [प्वाइंट ऑफ सेल]</p> <p>ई-कॉमर्स की परिभाषा- ई-कॉमर्स के मुख्य घटक, ई-कॉमर्स सुरक्षा के तत्व, ई-कॉमर्स सम्बन्धी खतरे, ई-कॉमर्स सुरक्षा सर्वोत्तम प्रथाएं, ऑनलाइन बिल भुगतान। डिजिटल भुगतान से संबंधित आम धोखाधड़ी और निवारक उपाय। आरबीआई के दिशानिर्देश और भुगतान निपटान अधिनियम, 2007 के प्रावधान।</p> <p>Keywords: <i>Internet Banking, Digital Financial Tools, eWallet, e-Commerce Security.</i></p>	08
III	<p>ई-गवर्नेंस सर्विस-</p> <p>रेलवे आरक्षण, पासपोर्ट, ई-अस्पताल जैसी ई-गवर्नेंस सेवाओं का अवलोकन; "उमंग ऐप" का उपयोग करके मोबाइल पर विभिन्न ई-गवर्नेंस सेवाओं तक पहुंचना। भारत सरकार के पोर्टल (https://www.mygov.in/) की सेवाओं और संसाधनों की खोज करना।</p> <p>डिजी-लॉकर: डिजिलॉकर के बारे में, डिजिलॉकर की विशेषताएं और लाभ, डिजिलॉकर पर विभिन्न प्रमाणपत्रों और मार्कशीट को पंजीकृत करना, एक्सेस करना और प्राप्त करना।</p> <p>अकादमिक बैंक ऑफ क्रेडिट (एबीसी): एबीसी का विवरण, एबीसी की विशेषताएं और लाभ, पंजीकरण, पहुंच, अकादमिक क्रेडिट प्राप्त करना और साझा करना।</p>	06

	<p>ऑनलाइन शिक्षण संसाधनों की खोज: SWAYAM Central (https://swayam.gov.in/) और ई-पाठशाला (https://epathshala.nic.in/) के माध्यम से ऑनलाइन शिक्षण।</p> <p>Keywords: <i>Internet Banking, NEFT, RTGS, IMPS, OTP, UPI, QR Code, AEPS, E-Governance, Umang.</i></p>	
IV	<p>साइबर सुरक्षा का परिचय-</p> <p>साइबरस्पेस का विनियमन, साइबर सुरक्षा की अवधारणा, साइबर सुरक्षा के मुद्दे और चुनौतियाँ।</p> <p>साइबर अपराध और उल्लंघनों की परिभाषा, कंप्यूटर और मोबाइल को लक्षित साइबर अपराध, महिलाओं और बच्चों के खिलाफ साइबर अपराध, साइबर बुलिंग। वित्तीय धोखाधड़ी, सोशल इंजीनियरिंग हमले, मेलवेयर और रैंसमवेयर हमले, जीरो डे और जीरो क्लिक अटैक।</p> <p>साइबर अपराधियों की कार्यप्रणाली-, साइबर अपराधों की रिपोर्टिंग, उपचारात्मक और शमन उपाय, साइबर अपराध का कानूनी परिप्रेक्ष्य, आईटी अधिनियम 2000 और इसके संशोधन, भारत में साइबर अपराध और साइबर सुरक्षा से निपटने वाले संगठन, केस स्टडी।</p> <p>Keywords: <i>Cyber Space, Cyber Security, Cyber Offences, Zero Click Attack, Zero Day Attack, Ransomware, Reporting Cyber Crimes, Cyber Crimes Case Studies.</i></p>	05
V	<p>सोशल मीडिया अवलोकन और सुरक्षा-</p> <p>सोशल नेटवर्क का परिचय, सोशल मीडिया के प्रकार, सोशल मीडिया प्लेटफॉर्म, सोशल मीडिया मॉनिटरिंग, हैशटैग, वायरल कंटेंट, सोशल मीडिया मार्केटिंग, सोशल मीडिया प्राइवैसी, ऑनलाइन सोशल नेटवर्क में चुनौतियाँ, अवसर और नुकसान, सोशल मीडिया से संबंधित सुरक्षा मुद्दे, फ्लैगिंग और अनुपयुक्त सामग्री की रिपोर्टिंग, अनुपयुक्त सामग्री पोस्ट करने के संबंध में कानून, सोशल मीडिया के उपयोग के लिए प्रथाएं, केस स्टडी।</p> <p>Keywords: <i>Social Media Platforms, Hashtagging, Social Media Marketing, flagging of contents in social media.</i></p>	06

भाग स-अनुशंसित अध्ययन संसाधन

पाठ्य पुस्तकें, संदर्भ पुस्तकें, अन्य संसाधन

अनुशंसित सहायक पुस्तकें /ग्रन्थ/अन्य पाठ्य संसाधन/पाठ्य सामग्री:

Suggested Readings:

- Praveen Kumar Shukla, Surya Prakash Tripathi, Ritendra Goel "Introduction to Information Security and Cyber Laws" Dreamtech Press.
- Vivek Sood, "Cyber law simplified", Tata McGrawHill, Education (India).
- T. Bradley "Essential Computer Security: Everyone's Guide to Email, Internet, and Wireless Security".
- Cyber Crime Impact in the New Millennium, by R. C Mishra , Auther Press. Edition 2010.
- Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd. (First Edition, 2011)
- Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform. (Pearson , 13th November, 2001)
- Electronic Commerce by Elias M. Awad, Prentice Hall of India Pvt Ltd.
- Cyber Laws: Intellectual Property & E-Commerce Security by Kumar K, Dominant Publishers.

- Network Security Bible, Eric Cole, Ronald Krutz, James W. Conley, 2nd Edition, Wiley India Pvt. Ltd.
- Fundamentals of Network Security by E. Maiwald, McGraw Hill

Reference Books:

- M. Stamp, “Information Security: Principles and Practice”, Wiley.
- David J. Loundy, “Computer Crime, Information Warfare, And Economic Espionage”, Carolina Academic Press.

अनुशंसित समकक्ष ऑनलाइन पाठ्यक्रम:

Suggested equivalent online courses: e-reading:

- <http://egyankosh.ac.in/handle/123456789/9489>
- https://workspace.google.com/intl/en_in/training/
- <https://www.classcentral.com/course/openlearn-science-maths-technology-preparing-your-96104>
- <https://www.udemy.com/course/free-computer-literacy-101-course/>
- <https://www.mygov.in/>
- <https://epathshala.nic.in/>
- <https://www.digilocker.gov.in/>
- <https://www.abc.gov.in/>
- <https://swayam.gov.in/>

भाग द - अनुशंसित मूल्यांकन विधियां:

अनुशंसितसतत मूल्यांकन विधियां:

अधिकतम अंक: 50

विश्वविद्यालयीनपरीक्षा (UE) अंक:50

आकलन : विश्वविद्यालयीन परीक्षा: समय- 01.00 घंटे	वस्तुनिष्ठ प्रश्न - 50	50
---	------------------------	----

कोई टिप्पणी/सुझाव: