5	Utilize knowledge of this course to design functional website using web design software	10%

List of Open learning website:

1. https://www.tutorialspoint.com/wordpress/index.htm
2. https://www.coursera.org/projects/build-a-full-website-using-wordpress

List of Open Source Software: ------- NIL ----------

FOR LAB SESSIONS: NA

List of Experiments: ------ NIL----

Major Equipment Needed: ----------NIL --------

Year: II (Sem IV)

Subject Name: Introduction to Cyber Security **Subject Code:** BTCO18201
Type of course: TransDisciplinary
Prerequisite: -

List of Courses where this course will be prerequisite: Cyber Security & Cyber Laws

Rationale: In the growing digital age, we have become more dependent on the internet for many of our daily activities. There are advantages and disadvantages of using the internet. Every day we see new cyber crime being reported. This course will provide awareness to deal with cyber crimes and take precautions to remain safe.

Teaching and Examination Scheme:

TEACHING SCHEME				Theory Marks			Practical Marks		Total
L	T	P	C	TEE	CA1	CA2	TEP	CA3	

2	0	0	0	0	0	50	0	0	50

CA1: Continuous Assessment (assignments/projects/open book tests/closed book tests CA2: Sincerity in attending classes/class tests/ timely submissions of assignments/self-learning attitude/solving advanced problems TEE: Term End Examination TEP: Term End Practical Exam (Performance and viva on practical skills learned in course) CA3: Regular submission of Lab work/Quality of work submitted/Active participation in lab sessions/viva on practical skills learned in course

Content:

Sr. No.	Content	Total Hrs
1	Importance of Cyber Security : Introduction and Definition of Cyber Security, Comparison of Cyber Security and Information Security, Objectives of Cyber Security, Cyber Security Roles and Governance, Domains of Cyber Security, Types of Cyber Crimes	4
2	Identity Theft: Definition of Identity Theft, Hacking or Gaining Access to Social Media Accounts, Misuse of Photocopy of Identity Proofs, Credit-Debit Skimming, Case Studies	4
3	Psychological Tricks: Introduction to Psychological Tricks, Phishing, Vishing, Smishing, Credit-Debit Card Fraud, Lottery Fraud, Job related Fraud, Case Studies	5
4	Social Media Frauds: Types of Social Media Fraud- Sympathy Fraud, Romance Fraud, Cyber Stalking, Cyber Bullying, Case Studies	4
5	Mobile Application Fraud: Use of Mobile Applications for Cyber Frauds, Cyber Attack using Infected Mobile Applications, Case Studies	4
6	Online Bank Frauds: Introduction, Digital Payment Application related Attacks, Hacking of Bank Accounts due to Weak Passwords, Hacking of Multiple Account due to Same Password, Case Studies	5
7	Virus Attack: Virus Attack on PC/Laptops, Virus Attack through External Devices, Virus Attack by Downloading File from Untrusted Websites, Virus Attack by Installing of Malicious Softwares, Case Studies, General Tips for Safety, Incident Reporting	4

Suggested Specification table with Marks (Theory): (For B.Tech only)

Distribution of Theory Marks					
R Level	**U Level**	**A Level**	**N Level**	**E Level**	**C Level**
20	20	10	0	0	0

Legends: R: Remembrance; U: Understanding; A: Application, N: Analyze and E: Evaluate C: Create and above Levels (Revised Bloom's Taxonomy)

Note: This specification table shall be treated as a general guideline for students and teachers. The actual distribution of marks in the question paper may vary slightly from above table.

Reference Books:

Sr No	Title of book /article	Author(s)	Publisher and details like ISBN	Year of publication	Publication Edition
1	Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives	Nina Godbole and Sunit Belpure	Wiley		Latest Edition
2	Cyber Security and Cyber Laws Paperback	Alfred Basta, Nadine Basta , Mary Brown, Ravinder Kumar	Cengage	2018	
3	Cybersecurity: The Beginner's Guide: A Comprehensive Guide to Getting Started in Cybersecurity	Erdal Ozkaya	Packt	2019	

Course Outcomes (CO):

Sr. No.	CO statement	Marks % weightage
1	Identify key concepts and terminology in cyber security.	20%
2	Understand various vulnerabilities and cyber attacks.	20%
3	Differentiate between types of cyber crimes.	20%
4	Identify everyday cyber frauds and take precautions to remain safe.	30%
5	Utilize knowledge of this course to protect themselves and society against Cyber Attacks.	10%

List of Open learning website:

1. https://onlinecourses.swayam2.ac.in/nou19_cs08/preview
2. https://www.coursera.org/specializations/intro-cyber-security