Introduction to Cyber Security

Welcome to the "Introduction to Cyber Security" course at St. Bede’s College. This undergraduate course is designed for first-year students across all streams, providing essential knowledge and practical skills for navigating the digital world safely. With 45 lectures and 3 credits, it covers fundamental concepts, practical applications, and project-based learning.

Course Overview and Objectives

This course aims to equip students with a foundational understanding of cyber threats and digital safety. We emphasize promoting responsible online behavior and fostering digital citizenship. Students will gain practical skills to identify and prevent common cyber threats, preparing them for a secure online presence.

A key objective is to encourage teamwork through awareness projects and the effective use of cyber tools. The course is delivered in English, with optional bilingual support in Hindi to ensure accessibility for all students.

Understand Cyber Threats

Grasp fundamentals of digital safety.

Promote Responsible Behavior

Cultivate digital citizenship.

Gain Practical Skills

Identify and prevent common threats.

Encourage Teamwork

Collaborate on awareness projects.

Unit 1: Fundamentals of Cyber Security

Unit 1, spanning Lectures 1-10, introduces core cyber security concepts. Students will learn about various types of threats, including Malware, Phishing, and Ransomware. We will also cover essential topics like data privacy, confidentiality, and an overview of the IT Act 2000 and Cyber Law, alongside basics of computer networking.

Practical sessions will focus on detecting phishing emails and performing antivirus installations and scans, providing hands-on experience with fundamental security measures.

Syllabus Highlights

- Introduction to Cyber Security
- Types of threats (Malware, Phishing, Ransomware)
- Data Privacy & Confidentiality
- IT Act 2000 & Cyber Law Overview
- Basics of Computer Networking

Practical Applications

- Detect phishing emails
- Install antivirus and perform scans

Unit 2: System & Network Security

Unit 2, covered in Lectures 11-20, delves into system and network security. Key topics include creating strong passwords and understanding various authentication methods. We will explore the roles of Firewalls, VPNs, and Proxy Servers in securing networks, and discuss different types of attacks such as DDoS, Brute Force, and MITM.

The unit also covers Wi-Fi security and the basics of cryptography. Practical exercises involve configuring firewalls and VPNs, and encrypting/decrypting basic text to reinforce theoretical knowledge.

Passwords & Authentication

Create strong passwords.

Firewalls & VPNs

Configure network defenses.

Attack Types

Understand DDoS, Brute Force, MITM.

Wi-Fi Security

Secure wireless connections.

Unit 3: Digital Hygiene & Responsible Use

Lectures 21-30, forming Unit 3, focus on digital hygiene and responsible online behavior. Students will learn safe browsing techniques and how to manage mobile app permissions, including awareness of OTP frauds. The unit also addresses critical issues like identity theft, social engineering, cyberbullying, and sextortion, along with reporting mechanisms.

Emphasis is placed on understanding and configuring social media privacy settings. Practical sessions include enabling two-factor authentication (2FA), analyzing privacy settings, and safely simulating OTP fraud scenarios.

Key Topics

- Safe Browsing Techniques
- Mobile App Permissions & OTP Frauds
- Identity Theft & Social Engineering
- Cyberbullying & Reporting Mechanisms
- Social Media Privacy Settings

Hands-on Practice

- Enable 2FA on accounts
- Analyze privacy settings
- Simulate OTP fraud (demo)

Unit 4: Cyber Tools & Simulations

Unit 4, covered in Lectures 31-40, introduces students to essential cyber tools and simulations. This includes an overview of ethical hacking concepts, focusing on tools like Wireshark and Nmap (demo use only). Students will learn about network monitoring using Task Manager and Netstat, and gain knowledge in data backup and recovery strategies.

A significant part of this unit involves engaging with Google Interland for cyber safety simulations. Practical exercises include using Wireshark to analyze packets, performing port scans with Nmap (demo only), and backing up data to cloud services or USB drives.

Ethical Hacking Overview

Introduction to concepts.

Kali Linux Tools

Wireshark, Nmap demos.

Network Monitoring

Task Manager, Netstat.

Data Backup & Recovery

Strategies for data protection.

Unit 5: Project Work & Revision

The final Unit 5, spanning Lectures 41-45, is dedicated to project work and revision. Students will engage in a group project, choosing from a variety of options designed to apply their learned skills in a practical context. These projects encourage creativity and collaboration, reinforcing the course objectives.

Options include developing a college-wide cyber safety campaign, conducting surveys on student digital habits, analyzing real-world cyber crime case studies in the Indian context, creating a comprehensive cyber safety handbook, or designing a secure social media profile.

Group Project Options

- College-wide Cyber Safety Campaign
- Survey on students' digital habits
- Case Study on a real cyber crime (Indian context)
- Create a Cyber Safety Handbook
- Design a secure social media profile

Learning Outcomes & Conclusion

Upon successful completion of this course, students will be able to recognize and prevent common cyber threats effectively. They will develop safe digital practices for personal and professional use, and gain proficiency in operating basic cyber security tools. Furthermore, students will be equipped to engage in peer-based cyber awareness initiatives, contributing to a safer digital community.

This course provides a comprehensive foundation for navigating the complexities of the digital world securely and responsibly.

Recognize & Prevent Threats

Identify common cyber threats.

Develop Safe Practices

Cultivate secure digital habits.

Operate Basic Tools

Utilize fundamental cyber security tools.

Engage in Awareness

Promote peer-based cyber awareness.