Course Goal: To provide beginners with a fundamental understanding of cybersecurity principles and introduce them to the basic ways Artificial Intelligence is being used in this field.

Target Audience: Individuals with no prior cybersecurity background, students exploring career options, and anyone interested in understanding digital safety and the role of AI in it.

Prerequisites: Basic computer literacy and internet usage.

Tools & Platforms (conceptual and user-friendly examples): Introduction to basic security settings on personal devices and online accounts, awareness of common AI-powered security features in everyday tools (e.g., spam filters, facial recognition).

Day 1: Introduction to the Digital World and Its Risks (1.5 Hours)

(**0-20 minutes) Our Digital Lives:**

- How much we rely on the internet and digital devices.
- Understanding personal data and its value.
- Common online activities and their potential risks (social media, online shopping, banking).
- Relevance to the digital landscape in Hyderabad and India.

(20-50 minutes) Basic Cybersecurity Concepts:

- What is Cybersecurity? Keeping information and systems safe.
- Core principles: Confidentiality (keeping secrets), Integrity (keeping data accurate), Availability (making sure systems work).
- Introduction to common threats: Viruses, malware, phishing (simple explanations).

(50-90 minutes) Protecting Yourself Online - Basic Hygiene:

- Creating strong passwords and using password managers (conceptual).
- Understanding and enabling Multi-Factor Authentication (MFA).
- Recognizing and avoiding common scams and phishing attempts.
- Keeping software updated on personal devices.

Day 2: Introduction to Artificial Intelligence - The Basics (1.5 Hours)

(0-30 minutes) What is Artificial Intelligence (AI)?

- AI in everyday life: Examples like virtual assistants, recommendation systems, facial recognition.
- Basic concepts: Machines learning from data, making decisions or predictions.
- Simple explanation of Machine Learning (ML) as a subset of AI.

(30-60 minutes) How AI Learns - Simple Analogies:

- Training AI with examples (like teaching a child).
- Recognizing patterns using AI.
- Introduction to the idea of algorithms (step-by-step instructions for AI).

(60-90 minutes) AI in Security - A Gentle Introduction:

- How AI can help identify unusual activity (like a security guard noticing something out of place).
- Examples of AI being used to filter spam emails or detect fake online accounts (user-friendly examples).
- The idea that AI can learn to spot threats faster than humans in some cases.

Day 3: Common Cyber Threats and How AI Can Help (1.5 Hours)

(0-30 minutes) Understanding Malware (Viruses, Worms, Ransomware):

- What these types of threats are and what they can do.
- How they can spread and infect devices.
- Basic steps to prevent malware infections.

(30-60 minutes) AI for Detecting Malware:

- How AI can analyze files and programs to look for suspicious behavior.
- The idea of "behavioral analysis" by AI to catch new and unknown malware.
- Simple examples of AI-powered antivirus software features.

(60-90 minutes) Phishing and Social Engineering - Human Tricks:

- What phishing emails and social engineering are and how they work.
- Recognizing red flags in suspicious messages.
- Basic steps to avoid falling for these tricks.

Day 4: AI for Identifying Phishing and Scams (1.5 Hours)

(0-30 minutes) How AI Analyzes Emails and Messages:

- Using Natural Language Processing (NLP) to understand the text.
- Looking for suspicious words, grammar, and tone.
- Checking links and attachments for malicious signs.

(30-60 minutes) AI in Spam Filters and Email Security:

- How spam filters learn from millions of emails to identify unwanted messages.
- The role of AI in making spam filters more accurate.
- Awareness of AI-powered features in email providers.

(60-90 minutes) AI and Fake Account Detection on Social Media:

- How AI can identify patterns of fake or malicious accounts.
- Analyzing profile information, activity, and connections.
- Understanding the basics of how platforms try to combat bots and scams using AI.

Day 5: Basic Network Security and AI's Role (1.5 Hours)

(0-30 minutes) What is a Network? (Simple Explanation):

- How devices connect to the internet and each other.
- Introduction to the idea of network traffic.
- Basic concepts of Wi-Fi security.

(30-60 minutes) Firewalls - Your Digital Gatekeeper (Basic Concept):

- What firewalls do: Controlling what traffic can enter and leave a network.
- Basic settings on home routers.
- The idea of AI helping firewalls learn and adapt to new threats.

(60-90 minutes) Intrusion Detection - AI Looking for Trouble:

- The concept of systems that monitor network traffic for suspicious activity.
- How AI can analyze network patterns to detect potential attacks (basic idea).
- Examples of AI helping to identify unusual network behavior.

Day 6: Protecting Your Devices and Data with AI Assistance (1.5 Hours)

(0-30 minutes) Endpoint Security (Protecting Laptops, Phones, etc.):

- The importance of antivirus software.
- Basic security settings on operating systems and mobile devices.
- Keeping apps updated for security.

(30-60 minutes) AI in Antivirus and Endpoint Protection:

- How modern antivirus uses AI to identify new threats.
- Behavioral analysis by AI to detect malicious software even if it's unknown.
- The concept of AI-powered "next-generation" antivirus.

(60-90 minutes) Data Privacy and AI:

- Basic concepts of data privacy and why it matters.
- How AI is used in some tools to help protect your privacy (e.g., identifying tracking).
- Awareness of privacy settings on online platforms.

Day 7: The Future of Cybersecurity and AI - Staying Safe (1.5 Hours)

(0-30 minutes) The Evolving Threat Landscape:

- How cyber threats are becoming more sophisticated.
- The increasing role of automation in attacks.
- The importance of continuous learning in cybersecurity.

(30-60 minutes) The Growing Role of AI in Security:

- AI as a crucial tool for defending against advanced threats.
- The potential for more intelligent and automated security systems.
- Understanding that both attackers and defenders are using AI.

(60-90 minutes) Staying Safe in the Age of AI:

- Reinforcing basic cybersecurity best practices.
- Being aware of new AI-powered threats and defenses.
- Resources for further learning about cybersecurity in India and globally.
- Q&A and course conclusion.