

ROBOTICS & AI

What is robotics technology?

Robotics in AI involves

integrating AI technologies into robotic systems to enhance their capabilities and enable them to perform more complex tasks.

In simple terms, robotics combines science, engineering, and technology to design, construct, operate, and use machines programmed to replicate, substitute, or assist humans in completing tasks of varying complexity. These machines are known as robots.

Who is the father of robotics?

The "Father of Robotics" is widely recognized as Joseph Engelberger.

He was an American physicist, engineer, and businessman who co-founded Unimation, the world's first robotics company, and is credited with developing the first industrial robot, the Unimate.

What is robotics and AI?

Robotics is the engineering field focused on designing, building, and operating robots, which are machines programmed to perform tasks autonomously or semi-autonomously.

Artificial intelligence (AI) is a broader field of computer science that aims to create systems capable of simulating human intelligence, including learning, problem-solving, and decision-making. While robotics can incorporate AI, it's not essential for all robots, as many are designed for simple, repetitive tasks.

CYBER SECURITY

What is Cyber Security?

Cybersecurity is the practice of protecting com-and data from unauthor-ized access, damage, or use, often referred to as cyberattacks. It encompasses a range of strategies, tech-nologies, and processes to safeguard di-gital assets, including hardware, software, and information.

Why is cybersecurity important?

Cybersecurity is crucial for protecting individuals, businesses, and governments from the increasing threats of cyberattacks. These attacks can have significant consequences, including financial losses, reputational damage, and data breaches.

Who needs cybersecurity?

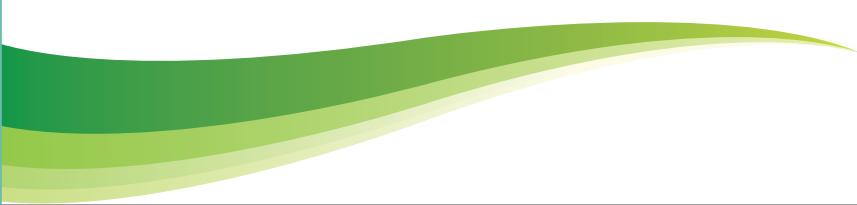
Everyone who uses technology needs to be concerned about cybersecurity, as individuals, businesses, and governments are all potential targets for cyberattacks.

In essence, cybersecurity is a multifaceted approach that combines technology, policy, and human behavior to protect digital assets from a variety of threats.

What is Cyber Crime?

In the context of cybersecurity. cybercrime refers to any illegal activity that targets or utilizes computers. networks, or the internet to commit a crime.

These crimes can range from stealing personal information to causing significant damage to systems and networks.



Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Most cybercrime is committed by cybercriminals or hackers who want to make money. However, occasionally cybercrime aims to damage computers or networks for reasons other than profit. These could be political or personal.

Cybercrime can be carried out by individuals or organizations. Some cybercriminals are organized, use advanced techniques and are highly technically skilled. Others are novice hackers.

What are the types of cybercrime?

Types of cybercrime include:

1. Email and internet fraud.
2. Identity fraud (where personal information is stolen and used).
3. Theft of financial or card payment data.
4. Theft and sale of corporate data.
5. Cyberextortion (demanding money to prevent a threatened attack).
6. Ransomware attacks (a type of cyberextortion)
7. Cryptojacking (where hackers mine cryptocurrency using resources they do not own).
8. Cyberespionage (where hackers access government or company data).
9. Interfering with systems in a way that compromises a network.
10. Infringing copyright.
11. Illegal gambling.
12. Selling illegal items online.
13. Soliciting, producing, or possessing child pornography.

Common Cyber Attacks You Should Know

Attack Type	What It Means		
<u>Phishing</u>	Phishing is a cyber attack where hackers trick users into revealing sensitive data like passwords, banking details, or session tokens through fake emails, messages, or websites. It uses <u>social engineering</u> to impersonate trusted sources and often includes malicious links or attachments to steal information.	<u>DDoS</u> (<u>Distributed Denial of Service</u>)	Hackers flood a website or server with too much traffic, so it slows down or crashes. It's like a traffic jam that blocks real users from getting in.

Every day, there are cyberattacks happening around the world.

Without basic protection, anyone—individuals or companies—can become a victim. That's why knowing about cybersecurity is just as important as locking your house.

In short, cybersecurity keeps your online world safe and secure.

It ensures that sensitive information remains confidential, intact, and accessible only to authorized users. Whether it's securing personal information, financial transactions, or corporate databases.