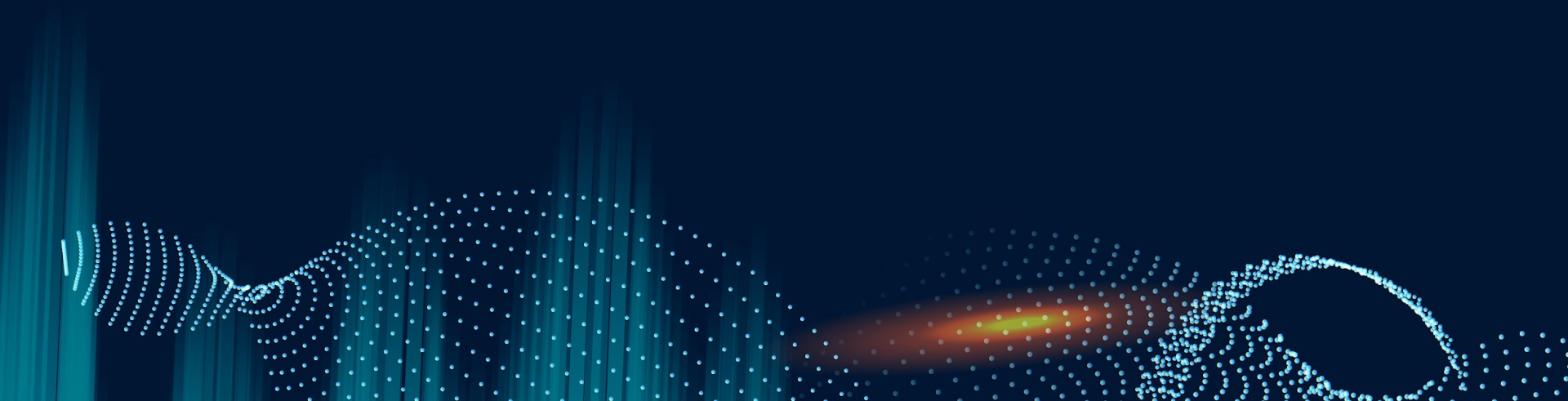
Cybersecurity

Session 5 : Fundamentals of Cybersecurity



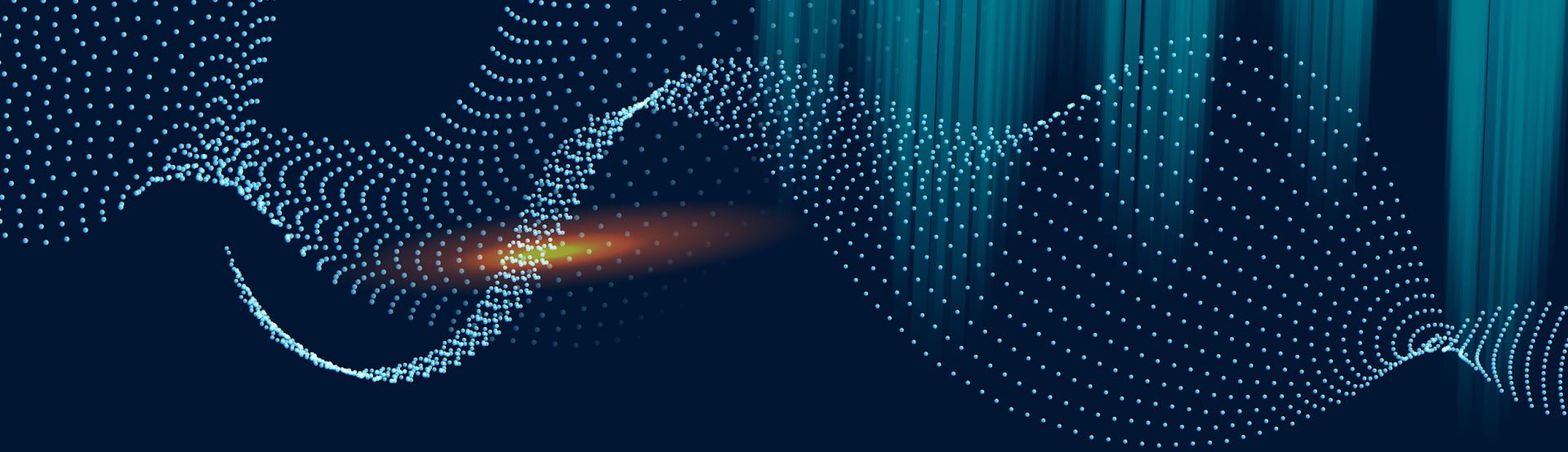
Fundamentals of Cybersecurity

01 What is cybersecurity?

02 Cyberthreats

03 Ethical Responsibility in Cybersecurity

04 Careers in Cybersecurity



01 What is cybersecurity?

What is cybersecurity?

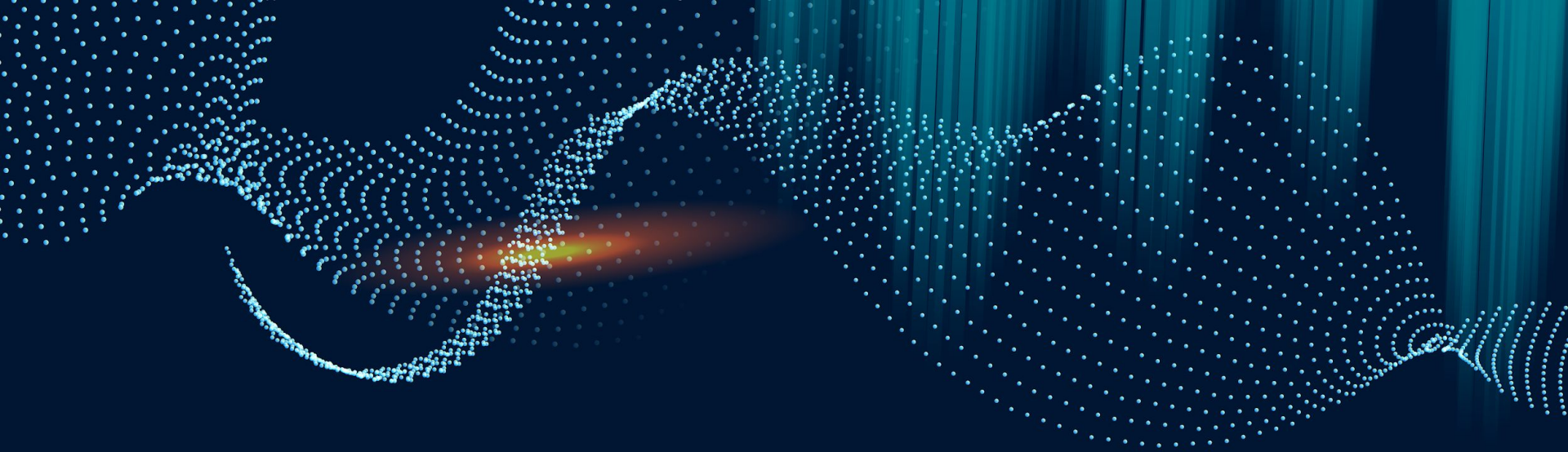
Cybersecurity involves the protection of digital systems, networks, devices, and data from unauthorized access, damage, or attack.

It's a critical component of modern digital life, covering everything from individual devices to large-scale networks and sensitive data.

What is Cybersecurity?

Why cybersecurity matters?

- Protection of personal information
- Help organizations build and maintain trust from their users/customers
- Prevention of financial loss
- Safety in daily online activities



02 Cyber Threats

Cyber Threats

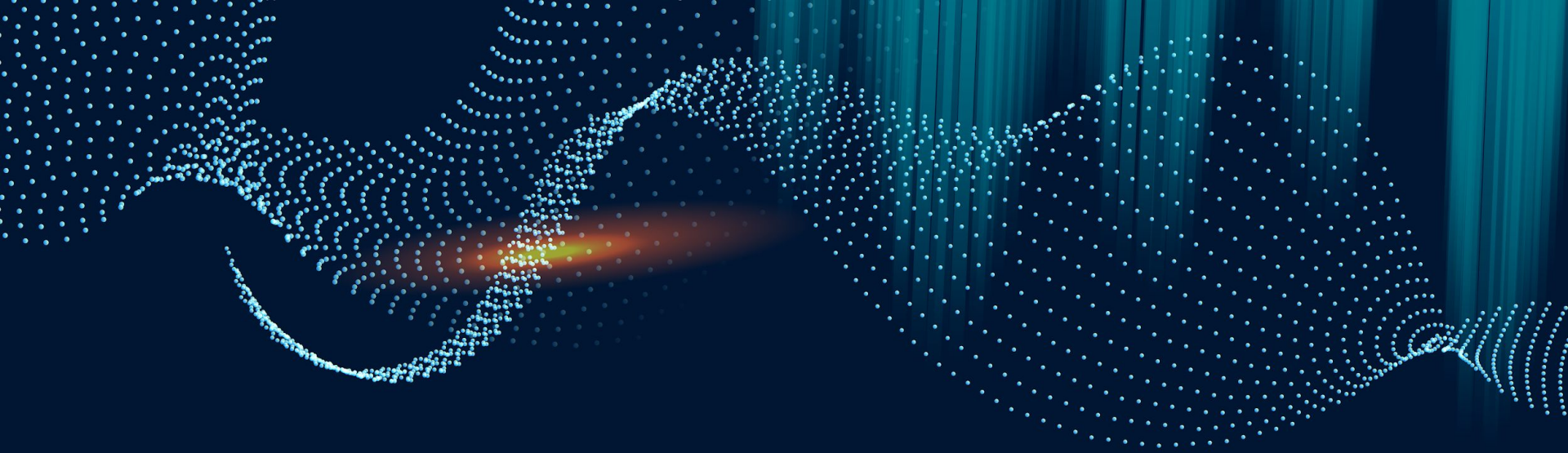
Types of cyber threats

- **Malware**: Malicious software like viruses, worms, trojans, and ransomware.
- **Phishing**: Social engineering attack to deceive users into providing sensitive information.
- **Man-in-the-Middle (MitM) Attacks**: Intercepting communications between two parties.
- **Denial of Service (DoS) Attacks**: Overloading systems to make services unavailable.

Cyber Threats

Basic cybersecurity measures

- **Using Strong Passwords:** How password length, complexity, and uniqueness protect against breaches.
- **Avoiding Suspicious Links:** Recognizing phishing links and emails.
- **Updating Software:** Patching vulnerabilities by keeping software up-to-date.
- **Two-Factor Authentication (2FA):** Adding an extra layer of security to accounts.



03 Ethical Responsibility in Cybersecurity

Ethical Responsibility in Cybersecurity

What is Ethical Hacking?

Ethical hacking, or penetration testing, involves authorized probing of systems to find vulnerabilities before malicious hackers can exploit them. Organizations utilize ethical hacking for vulnerability assessments and security audits to proactively address security weaknesses – it is crucial for compliance with regulations and for building robust security frameworks to mitigate cyber risks.

Components of Ethical Hacking

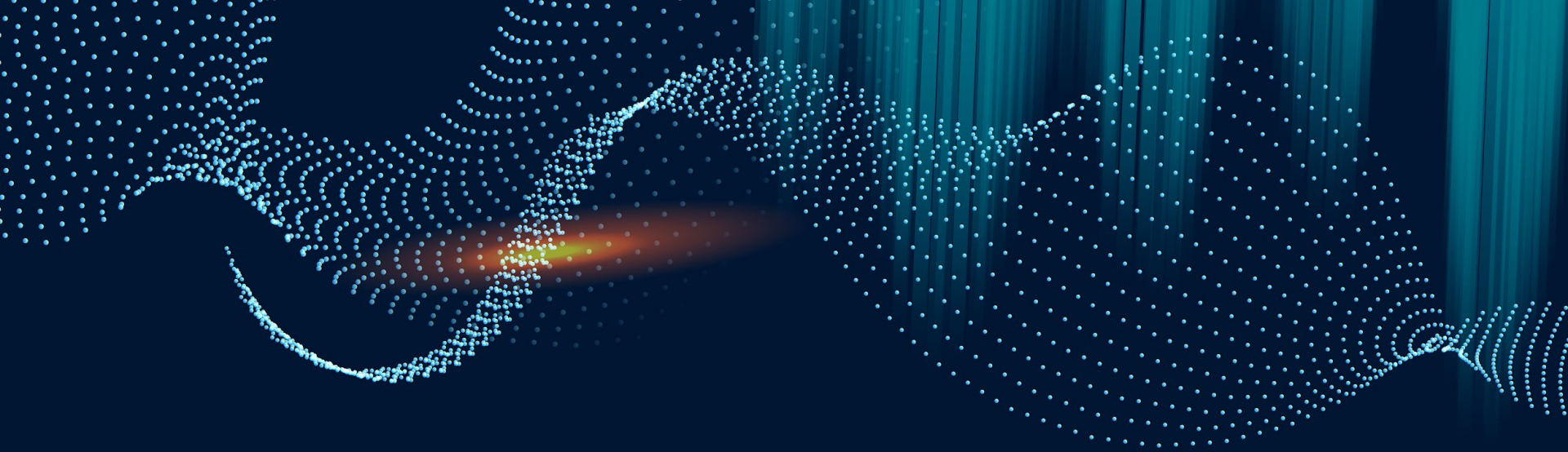
- Authorization
- Planning and Preparation
- Reconnaissance
- Exploitation
- Post-exploitation
- Reporting
- Remediation

Ethical Responsibility in Cybersecurity

Being a Responsible Internet User

Being a responsible internet user involves understanding and applying best practices to ensure a safe, respectful, and secure online experience. Below are some key aspects of responsible internet use:

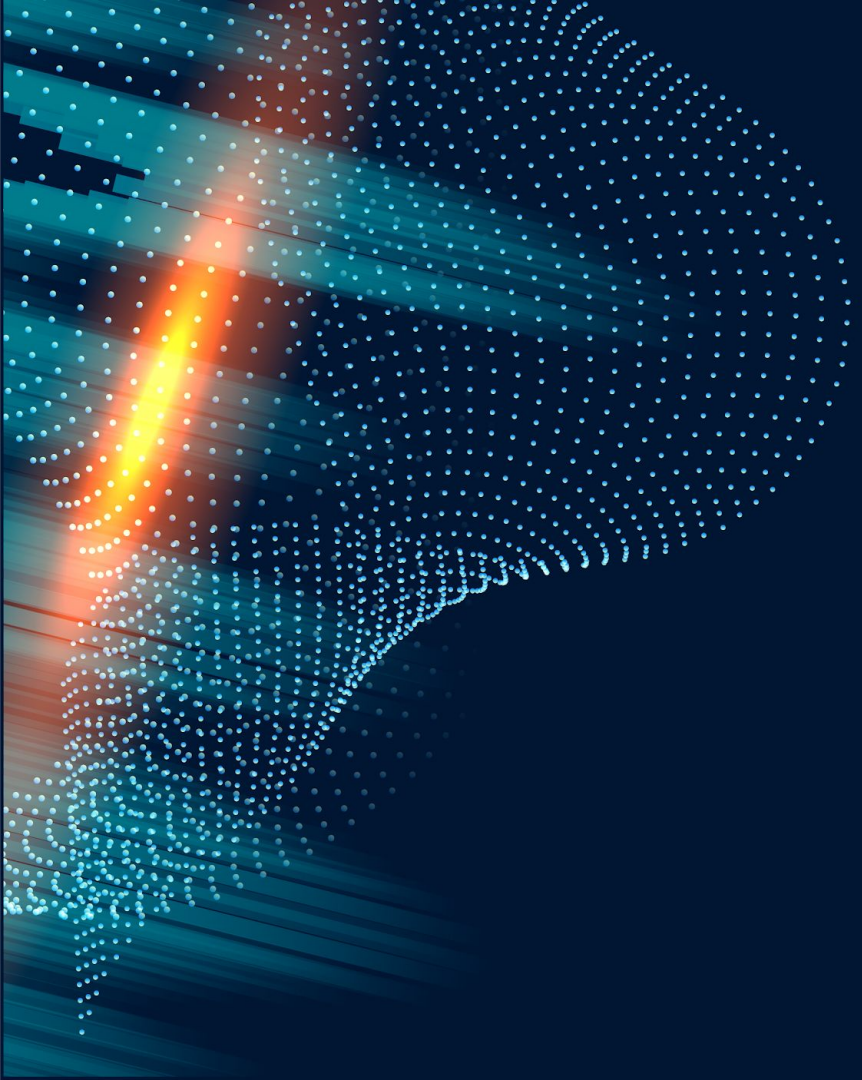
- Protecting personal information
- Using strong passwords
- Identifying and avoiding scams
- Practicing safe browsing habits
- Understanding digital footprints
- Educating yourself and others



04 Careers in Cybersecurity

Careers

- **Information Systems Security:** Managing security measures for organizations.
- **Network Security Administration:** Securing and monitoring networks to prevent unauthorized access.
- **Incident Response:** Responding to and mitigating cyberattacks.



Q&A