"ETHICS IN THE CYBER ERA: DEFENDING AGAINST DIGITAL THREATS"

Presented to-
Engr. Sheikh Tonmoy
Designation: Lecturer
Department of Software Engineering
Daffodil International University

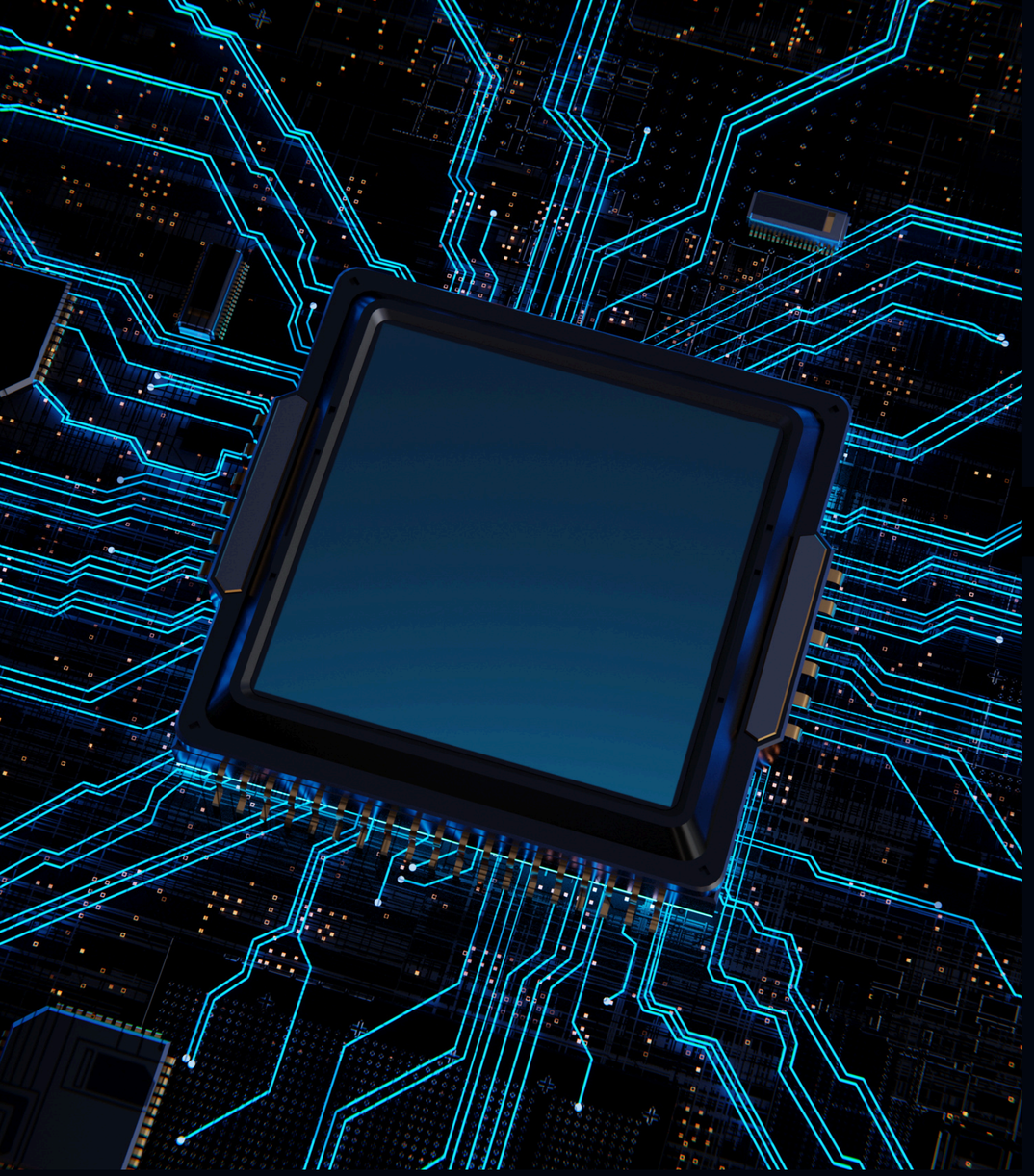
OUR AMAZING TEAMS

Md.Rufsanjani Shanto
Id: 221-35-1064

Razin Saleh
Id: 221-35-1055

Syeda Sadika Anjum
Id: 221-35-1066

Treebany Rani Saha
Id: 221-35-1061



INTRODUCTION

- Cybercrime is one of the most critical threats in today’s digital world.
- Software engineers have ethical responsibilities to protect users, systems, and data.

Focus of this presentation:

- Types of Cybercrime
- Real-world Examples
- Prevention Strategies
- Role of Professional Ethics

WHAT IS CYBER ETHICS?

DEFINITION: Moral principles governing technology use

Examples:

- Respecting privacy
- Avoiding cyberbullying
- Honesty in online activities

COMMON DIGITAL THREATS

Cybercrime

Hacking,Phishing, Ransomware

Social engineering

Tricking people into revealing information.

Data breaches

Theft of personal or corporate information.

Misinformation

Spreading false information for manipulation.

CYBERCRIME

Illegal activities carried out using computers, networks, or the internet.

- Affects individuals, businesses, and governments.
- Involves digital devices as targets or tools.

.

MAJOR TYPES OF CYBERCRIME

Types of Cybercrime

Examples of Cybercrime

WannaCry Ransomware (2017)

Infected 200,000+ computers worldwide

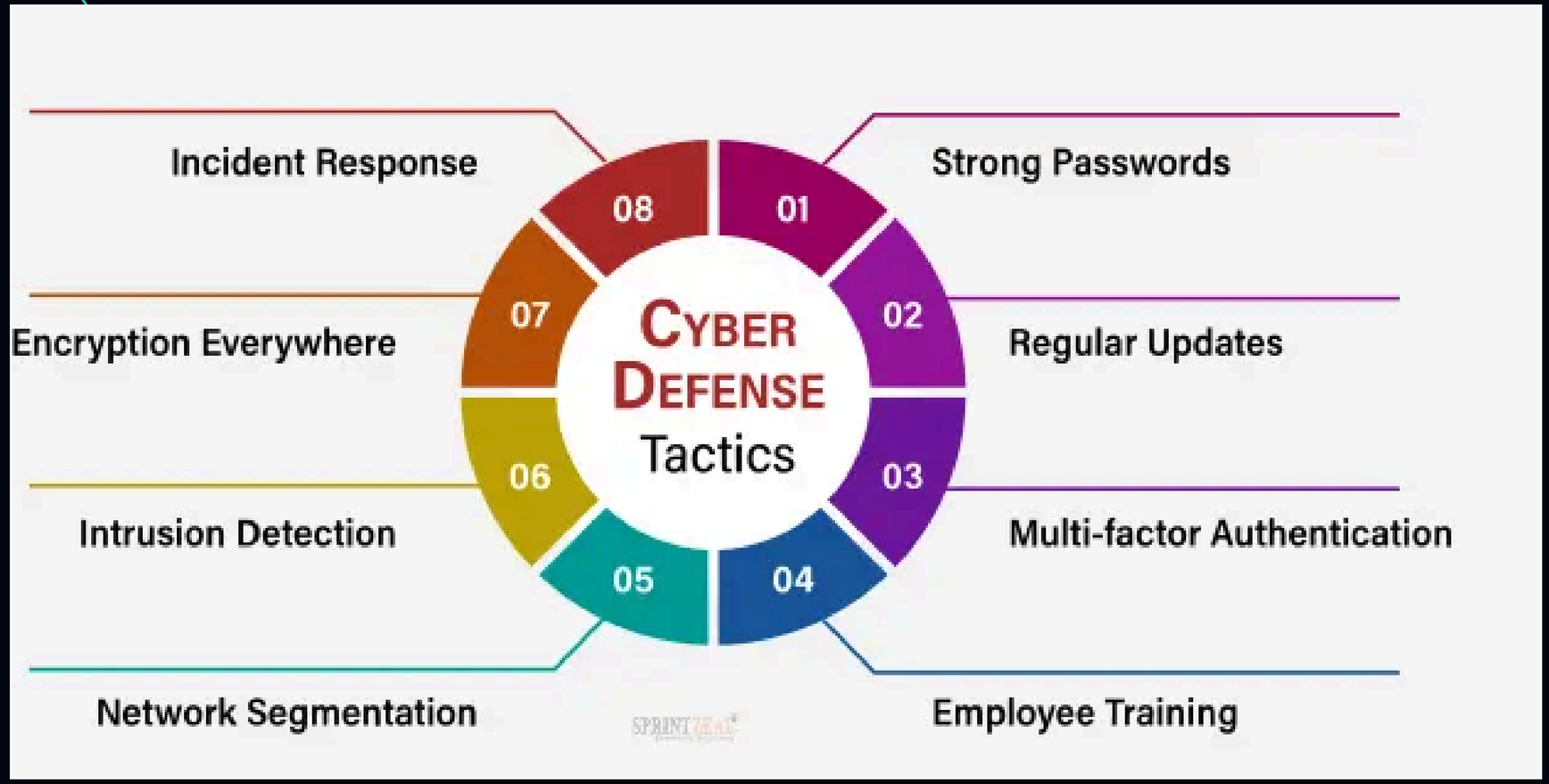
Equifax Data Breach (2017)

Stolen data of 147 million people

Yahoo Data Breach (2013–2014)

3 billion accounts affected

Prevention Strategies



PROFESSIONAL ETHICS IN CYBERSECURITY

Integrity :
Avoid exploiting security flaws

Confidentiality :
Protect user data.

Accountability :
Take responsibility for system failures.

Compliance :
Follow laws and regulations

ETHICAL DILEMMAS

- Should a software engineer report a vulnerability found in their company’s system?
- Is it ethical to track user activity for “security purposes” without consent?
- How to balance privacy vs public safety?

CASE STUDY

Case: Facebook–Cambridge Analytica Scandal (2018)

What happened: User data was harvested without consent for political profiling.

Ethical violation: Breach of privacy, misuse of data.

Lesson: Transparency, consent, and responsible data handling are crucial.

CONCLUSION

- Cybercrime is evolving — prevention requires technical and ethical action.
- Software engineers must act as ethical guardians of the digital world.
- Key takeaway: “Security without ethics is incomplete.”


Thank
you