

Course Title

Introduction to Cyber Security

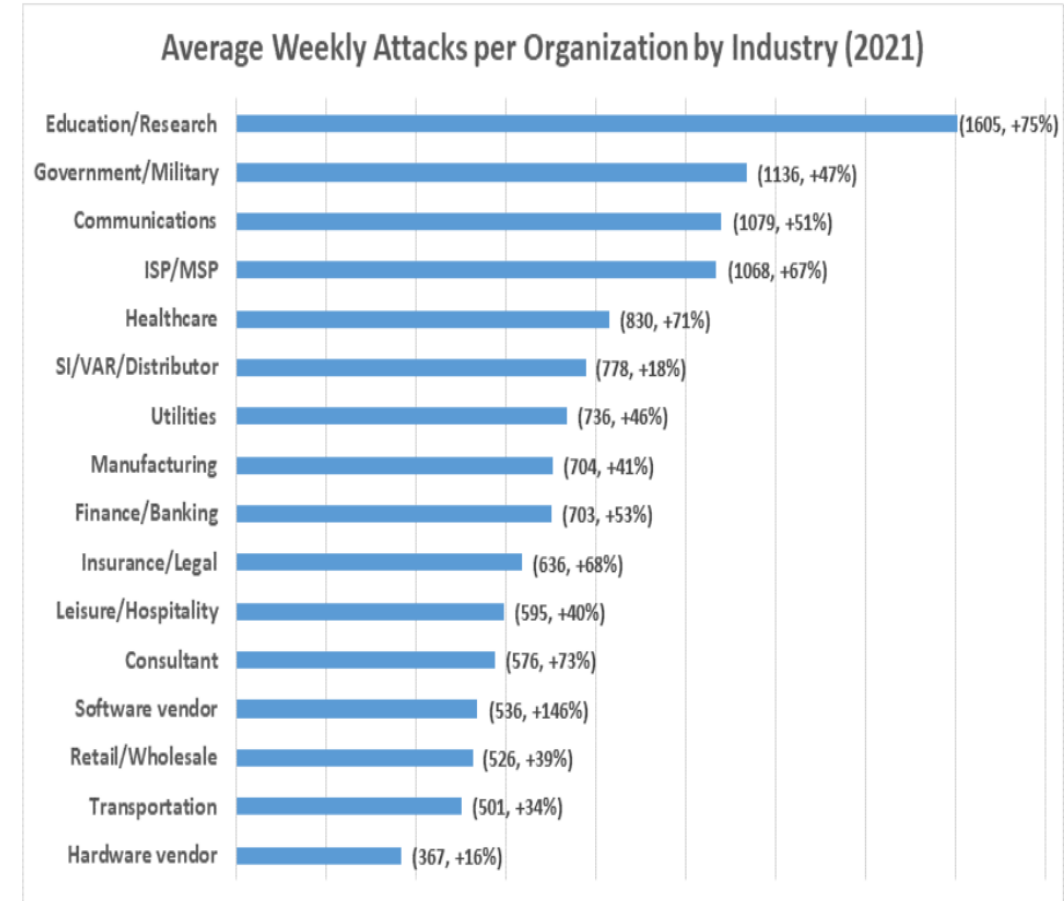
Course Code

22EM1C07

Host Dept

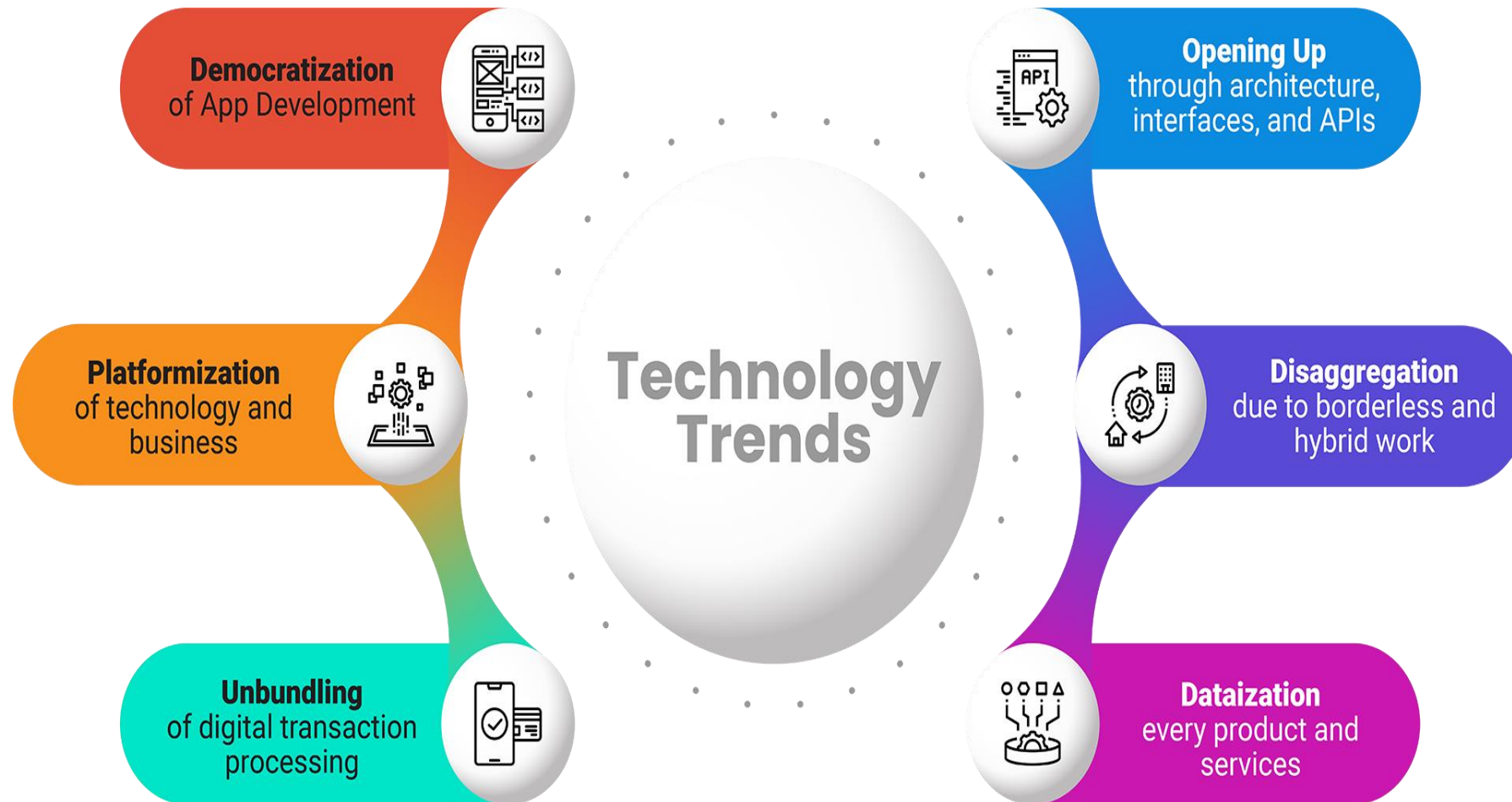
Computer Science & Engineering

- Practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.
- Data security and information protection
- **Growth and usage of internet**
- Covid-19
- Cyber Attacks Increased 50% Year over Year
- Application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber attacks.
- **Critical issue for every organization. It addresses people, processes and technology**
- Cyber security awareness



Source: <https://blog.checkpoint.com/2022/01/10/check-point-research-cyber-attacks-increased-50-year-over-year/>

# Why CyberSecurity?



## Major Cybersecurity Job roles, Job openings with Salary Package



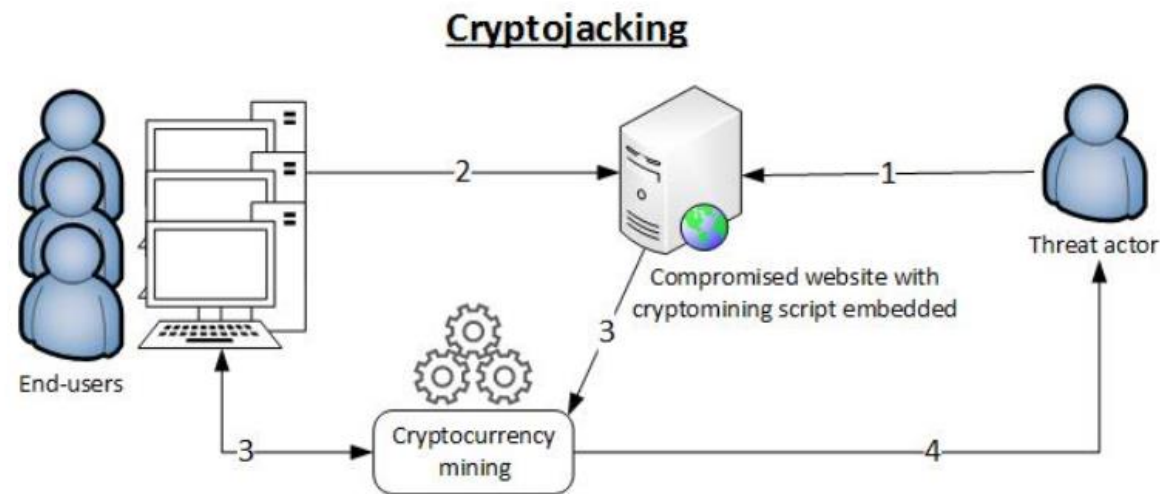


# What is Cyber Security



# CRYPTOJACKING

- Another party's **computing resources are hijacked** to mine cryptocurrency.
- Cryptojacking, which is also referred to as **malicious cryptomining**
- hackers mine cryptocurrency without paying for electricity, hardware and other mining resources.



**Steps**

1. The threat actor compromises a website
2. Users connect to the compromised website and the cryptomining script executes
3. Users unknowingly start mining cryptocurrency on behalf of the threat actor
4. Upon successfully adding a new block to the blockchain, the threat actor receives a reward in cryptocurrency coins



# What is Cyber Security



- Shodan is the world's first search engine for Internet-connected devices.
- Discover how Internet intelligence can help you make better decisions.



# What is Cyber Security

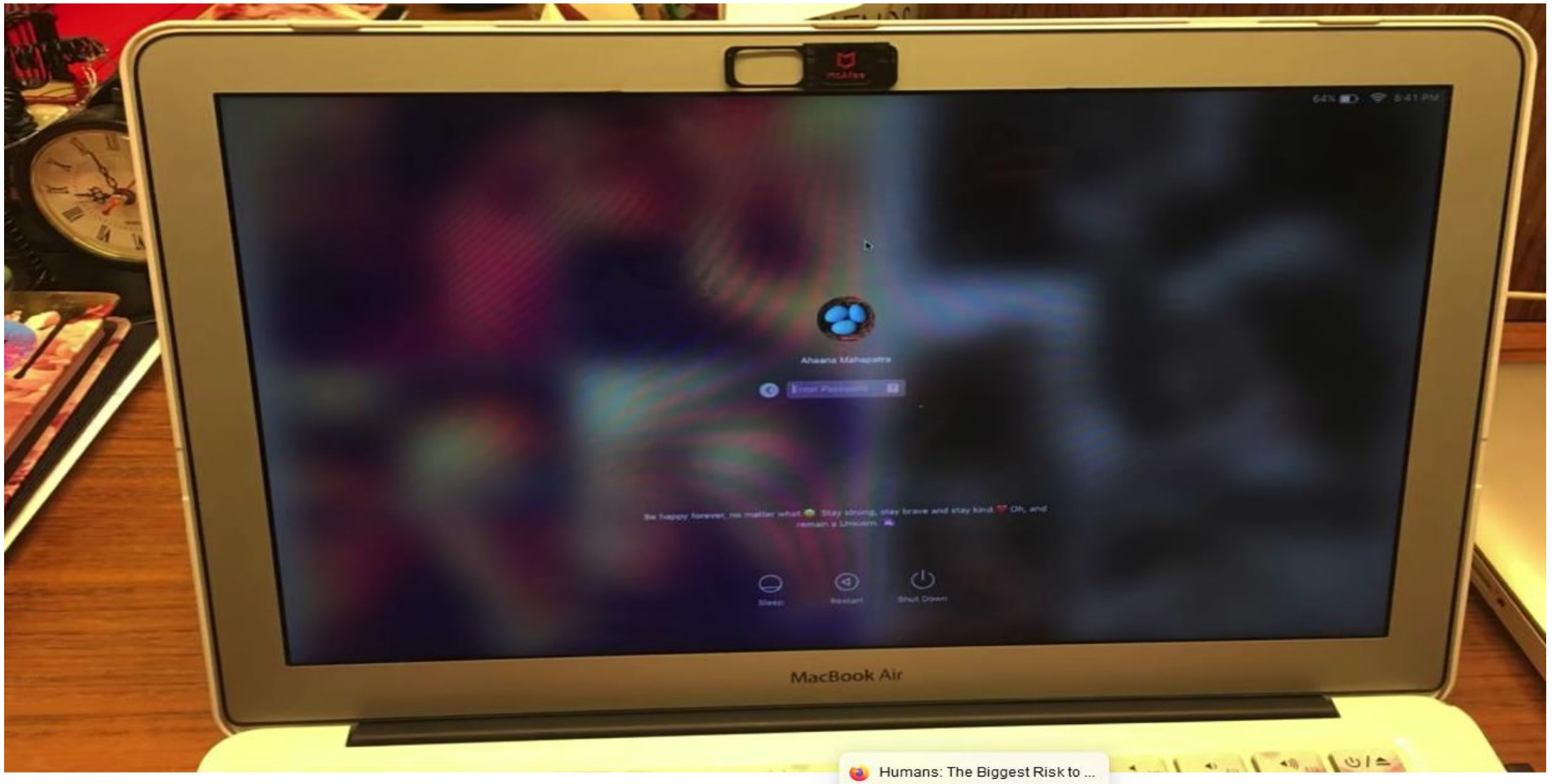


# What is Cyber Security



- The automation of systems **to detect and prevent cyber threats, while contributing to the overall threat intelligence of an organization in order to plan and defend against future attacks**
- Typical smart homes are **vulnerable to a high number of data attacks.**
- Reported instances of smart home attacks have included **hackers remotely controlling smart lights and smart TVs, unlocking IoT-enabled doors, and remotely turning on and streaming video from smart cameras**

# What is Cyber Security





# What is Cyber Security



<https://www.youtube.com/watch?v=8fQieCMoym0>



**OUR PASSWORD IS OUR IDENTITY**

Enter Password

**EasyToRemember**





## OUR PASSWORD IS OUR IDENTITY

Enter Password

**EasyToRememberButLong**



- Breaches of Last Few years:
- Sony Pictures: whole movie was Hacked
- Yahoo: 2billons records Hacked



- Biggest Data Breaches in US History [as on December 2022]

<https://www.upguard.com/blog/biggest-data-breaches-us>

- To create **awareness** with introductory course on cyber security through **discussion and simulations** on the basics, different models, cyber attacks, **legal and ethical aspects** and to enable to build cyber eco systems.

## Course Description and outline

**Unit 1 - Cyber Space, Cybercrime**

**Unit 2 - Cyber Offenses Attacker Techniques**

**Unit 3 - Social Media Overview and Security**

**Unit 4 - E - Commerce and Digital Payments**

**Unit 5 - Digital Devices security, Tools and Technologies for Cyber Security**

Unit-I	9 Hrs
<b>Introduction to Cyber Space</b> History of Internet, History and evolution of Information Security and cyber-Security, introduction to cyber space and information security, computer ethics and security policies.	
<b>Introduction to Cybercrime</b> Definition and Origins of the Word, Cybercrime and Information Security, who are Cybercriminals? Classifications of Cybercrimes, An Indian Perspective, Hacking and Indian Laws., Global Perspectives. Different Types of Cyber Crimes, Scams and Frauds	



Unit – II	9 Hrs
<b>Cyber Offenses</b> How Criminals Plan Them: Introduction, how criminals plan the attacks, Social Engineering, Cyber Stalking, Cybercaafe & cybercrimes, Botnets: The fuel for cybercrime, Attack Vector. <b>Attacker Techniques and Motivations:</b> How Hackers Cover Their Tracks (Anti-forensics), How and Why Attackers Use Proxies, Tunnelling Techniques, Fraud Techniques.	

Unit –III	9 Hrs
<b>Social Media Overview and Security</b> Introduction to Social networks. Types of social media, Social media platforms, Social media monitoring, Hashtag, Viral content, Social media marketing, Social media privacy, Challenges, opportunities and pitfalls in online social network, Security issues related to social media, Flagging and reporting of inappropriate content, Laws regarding posting of inappropriate content, Best practices for the use of social media, Case studies.	

**Unit -IV****9 Hrs****E - Commerce and Digital Payments**

Definition of E- Commerce, Main components of E-Commerce, Elements of E-Commerce security, E-Commerce threats, E-Commerce security best practices, Introduction to digital payments, Components of digital payment and stake holders, Modes of digital payments- Banking Cards, Unified Payment Interface (UPI), e-Wallets, Unstructured Supplementary Service Data (USSD), Aadhar enabled payments, Digital payments related common frauds and preventive measures. RBI guidelines on digital payments and customer protection in unauthorised banking transactions. Relevant provisions of Payment Settlement Act,2007

Unit-V	9 Hrs
<b>Digital Devices security, Tools, and Technologies for Cyber Security</b> End Point device and Mobile phone security, Password policy, Security patch management, Data backup, Downloading and management of third-party software, Device security policy, Cyber Security best practices, Significance of host firewall and Ant-virus, Management of host firewall and Anti-virus, Wi-Fi security, Configuration of basic security policy and permissions.	



- Fundamental **concepts and principles** in cyber security, distinguish among the **attacks**, **threats** and **vulnerabilities**
- Understand and apply different **cyber security techniques**
- Issues, challenges and guidelines for safe internet browsing, smart phone security, social media security, secure password, Wi-Fi security issues.
- To classify and explain different **types of security architectures** and **defense methods**
- To Identify, differentiate and explain **different cyber crimes and frauds**
- To Apply different **cyber crime investigation methods and techniques** for typical cases
- To Develop suitable **processes for forensic investigations**
- **Legal and ethical aspects in cyber laws** and employ them in typical cyber security cases taken for study.

<b>Course Outcomes: After completing the course, the students will be able to: -</b>	
<b>CO 1</b>	Understand the cyber-attacks and their principles for different domains - social media, E-commerce, and digital devices.
<b>CO 2</b>	Analyse vulnerabilities in different domains that the attacker capitalizes for attack.
<b>CO 3</b>	Apply different attacking techniques that make use of vulnerabilities available in various domains.
<b>CO 4</b>	Evaluate methods to cover different vulnerabilities to safeguard the systems against cyber-attacks.
<b>CO 5</b>	Investigate modern tools and technologies available to mitigate cybercrime attacks.

## Reference Books

- |    |   |
|----|---|
| 1. | Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd, 1 <sup>st</sup> Edition 2011, Reprint 2022, ISBN: 978-81-265-2179-1. |
| 2. | Cyber Security Essentials by James Graham, Richard Howard, Ryan Olson, CRC Press, 2011 Taylor and Francis Group. ISBN13: 978-1-4398-5126-5.   |
| 3. | Information Systems Security: Security Management, Metrics, Frameworks and Best Practices by Nina Godbole, 2 <sup>nd</sup> Edition, Wiley publishers, 2017. ISBN: 9788126564057.                                    |
| 4. | Network Security Bible, Eric Cole, Ronald Krutz, James W. Conley, 2nd Edition, John Wiley & Sons, 2005, ISBN: 978-0764573972.   |
| 5. | Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform, Pearson, 2001, ISBN: 9781516821020.                                |
| 6. | Electronic Commerce by Elias M. Awad, Pearson, 1st edition, 2001, ISBN: 978-0130193223.   |
| 7. | Cyber Laws: Intellectual Property & E-Commerce Security by Kumar K, Dominant Publishers & Distributors, 2011, ISBN: 978-8187336891.   |

- Basic necessity and need in HEI.
- UGC & AICTE.
- Educating family members, friends and to help society.
- Good Job opportunities with attractive high package



Source: <https://www.computercareers.org/cyber-security-salary/>

Cybersecurity specialist earns an average of \$45.33 per hour, monthly salary start from \$4,315 and go up to \$12,049. The average annual salary is \$94,290 and can go up to \$144,585.

Hourly Rate	Weekly	Monthly	Annual
\$45.33	\$1,813	\$7,858	\$94,290

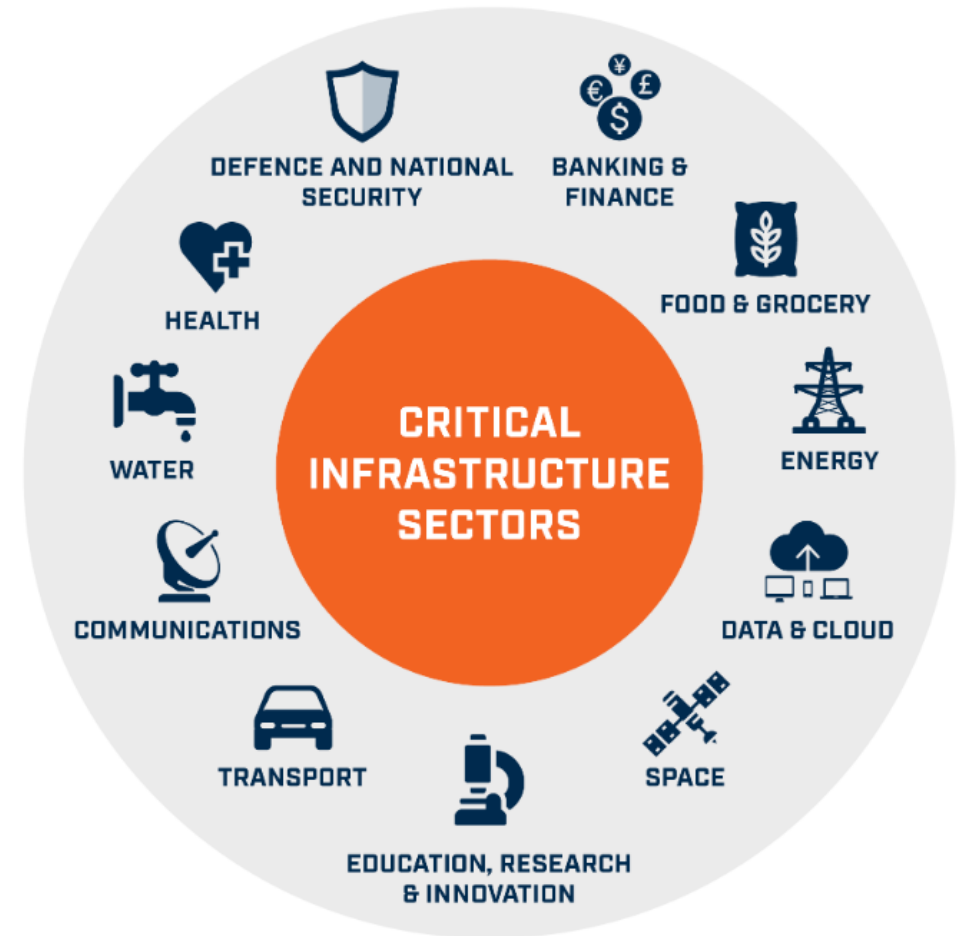
## Salary Range

Percentile	10%	25%	50%	75%	90%
Hourly	\$24.89	\$33.17	\$43.99	\$56.41	\$69.51
Weekly	\$996	\$1,327	\$1,760	\$2,256	\$2,780
Monthly	\$4,315	\$5,750	\$7,625	\$9,778	\$12,049
Annual	\$51,777	\$68,998	\$91,500	\$117,338	\$144,585

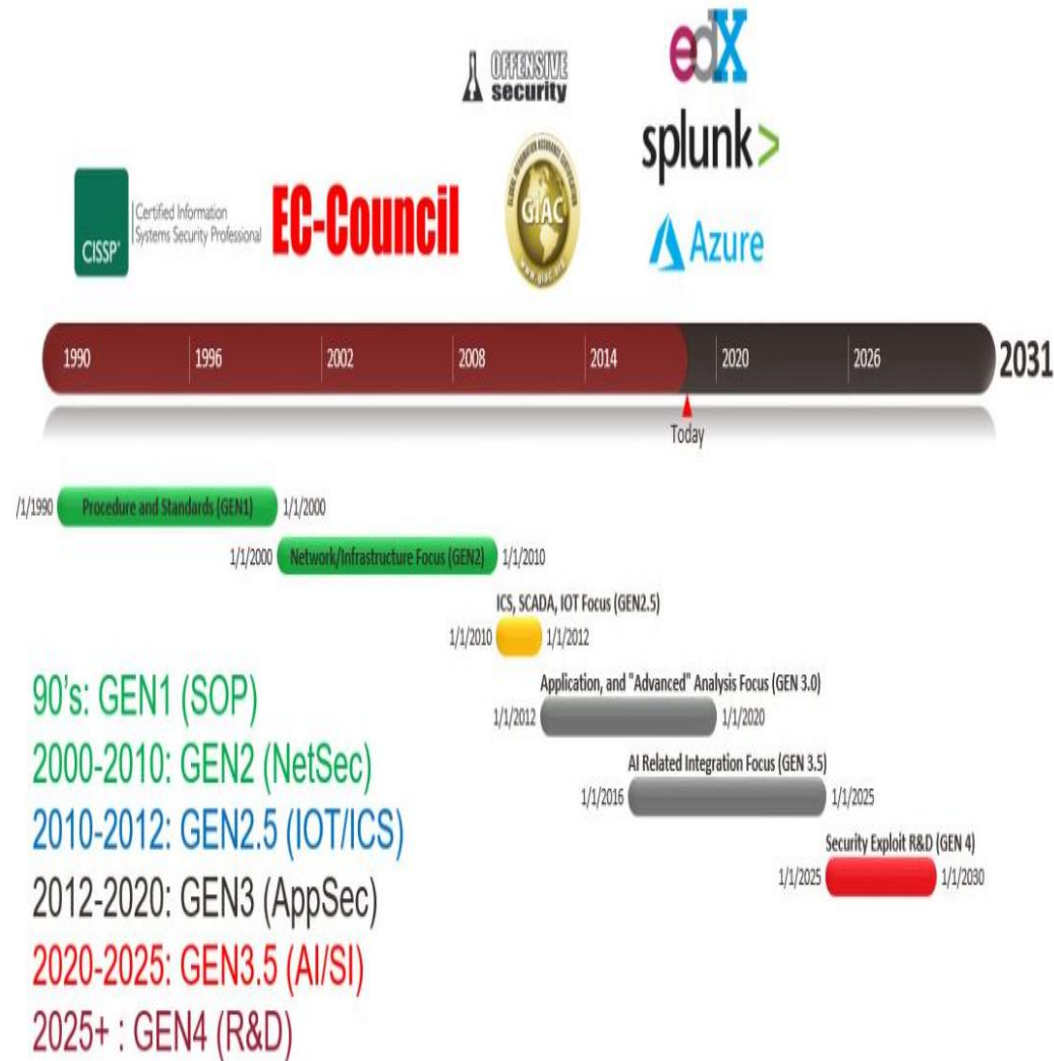
## career opportunities / Industry support

- Government and private organizations, Defence & Intelligence, Justice & Law Enforcement
- Telecommunications, Critical Infrastructure, Cloud & Online Services, Managed Security Serv
- Network/Application Security Analyst, Cyber Security Analyst
- Security Automation
- Cyber Security Practitioner
- Cyber Defense Analyst
- Penetration Tester
- Information Security Engineer in IT Industries
- Cyber Security Experts in in Governmental Organizations.
- Information Security Crime Investigator/Forensics Expert
- Information Security Analyst
- Lead Software Security Engineer
- Chief Information Security Officer (CISO)
- Security Architect
- CISSP – The Certified Information Systems Security Professional.
- CISM – Certified Information Security Manager.
- CISA – Certified Information Systems Auditor.
- GIAC – Global Information Assurance Certification.
- CEH – Certified Ethical Hacker.

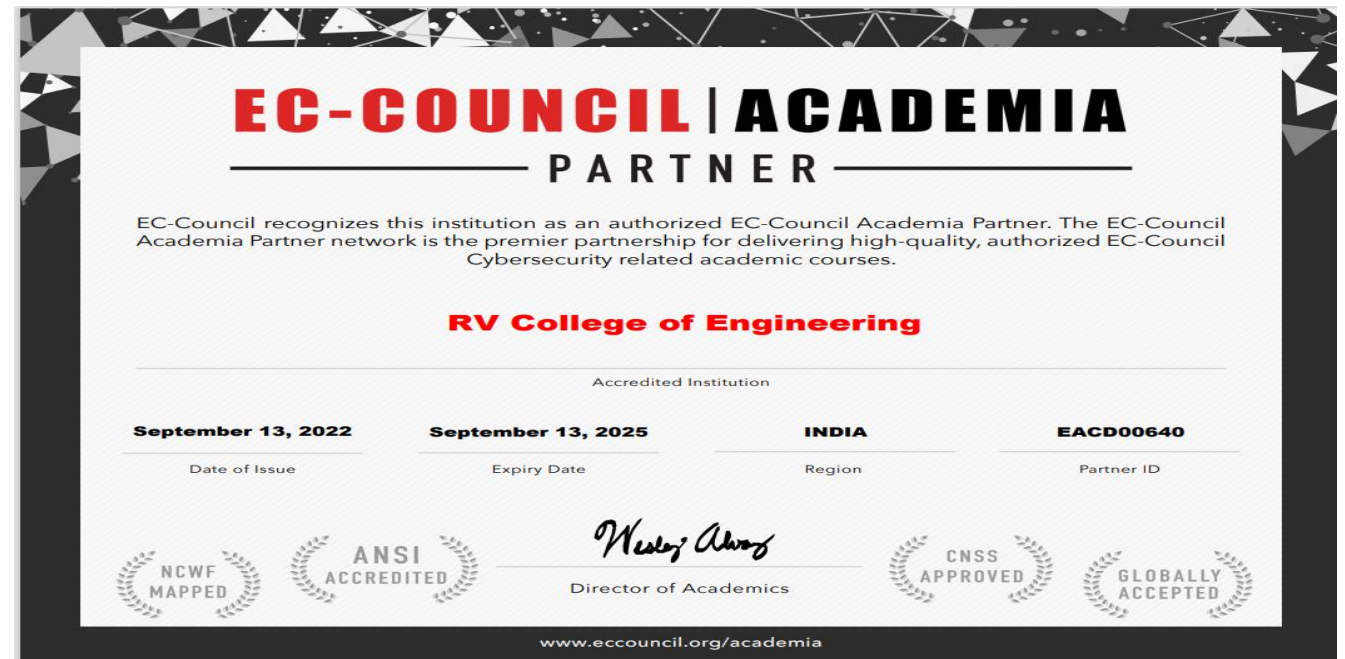
## Critical Infrastructure Cyber Security Solutions







- Leading cyber security certification bodies
- EC-Council (International Council of E-Commerce Consultants)
- CREST - the Council of Registered Ethical Security Testers



**Dr. Mohana****Assistant Professor****Computer Science and Engineering (Cyber Security)****Email (RVCE)****[mohana@rvce.edu.in](mailto:mohana@rvce.edu.in)****Office Number****Mobile****9739866723**