R.M.K GROUP OF ENGINEERING INSTITUTIONS

R.M.K GROUP OF INSTITUTIONS

R.M.K GROUP OF INSTITUTIONS

R.M.K GROUP OF INSTITUTIONS

Please read this disclaimer before proceeding:

This document is confidential and intended solely for the educational purpose of RMK Group of Educational Institutions. If you have received this document through email in error, please notify the system manager. This document contains proprietary information and is intended only to the respective group / learning community as intended. If you are not the addressee you should not disseminate, distribute or copy through e-mail. Please notify the sender immediately by e-mail if you have received this document by mistake and delete this document from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contentsof this informationisstrictlyprohibited.

22CS930 ENTERPRISE CYBER SECURITY

Department: CSE(CS)

Batch/Year: 2022-2026/IV

Created by: Dr. Udhaya Sankar S M

Professor & Head/CSE(CS)

Date: 15.5.2025

R.M.K GROUP OF INSTITUTIONS

1.TABLE OF CONTENTS

R.M.K GROUP OF INSTITUTIONS

R.M.K GROUP OF INSTITUTIONS

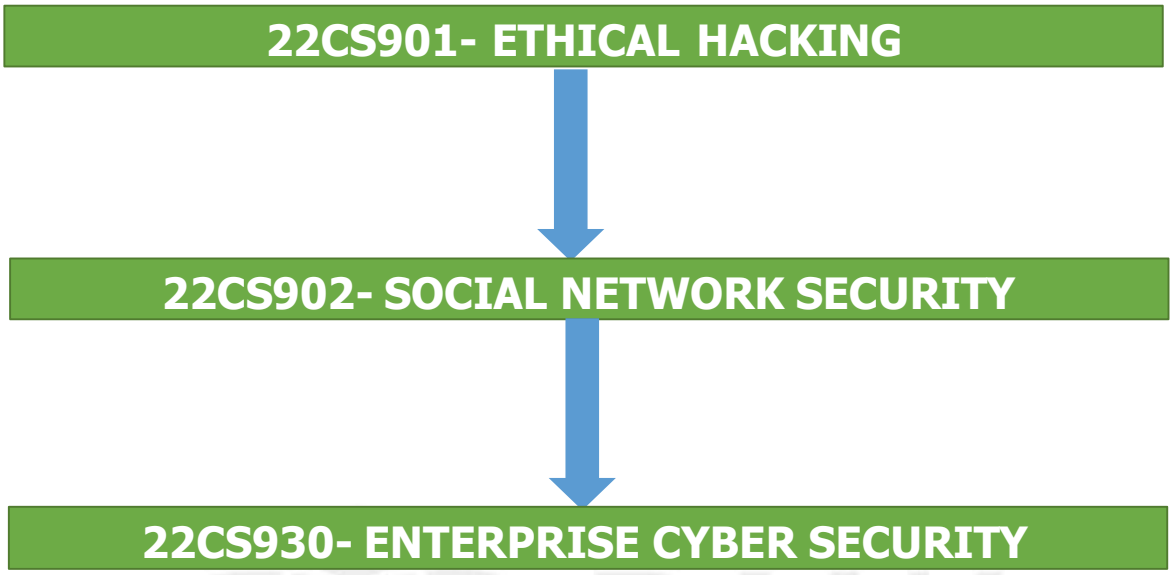
2. COURSE OBJECTIVES

- Learn the fundamentals of cryptography.
- Learn the key management techniques and authentication approaches.
- Explore the network and transport layer security techniques.
- Understand the application layer security standards.
- Learn the real time security practices.

R.M.K GROUP OF INSTITUTIONS

3. PRE REQUISITES

PRE-REQUISITE CHART



R.M.K GROUP OF INSTITUTIONS

4.SYLLABUS

22CS930- ENTERPRISE CYBER SECURITY

L	T	P	C
3	0	0	3

Unit-I INTRODUCTIONTOCYBERSECURITY 9

Cyber Security – Need of Cybersecurity in Organizations – CIA Triad- Confidentiality, Integrity, Availability; Reason for Cyber Crime –Need for Cyber Security – History of Cyber Crime; Cybercriminals – Classification of Cybercrimes– A Global Perspective on Cyber Crimes; Cyber Laws – The Indian IT Act – Cybercrime and Punishment.

Unit II : NETWORK SECURITY BASICS 9

Network Security Concepts- Basics of Networks- Common Types of Network Attacks- Introduction to Firewalls- Types of Firewalls- IDS/IPS- Virtual Private Networks (VPN's)- Secure configuration and management of network devices. Case Study: Install Kali Linux on Virtual box.

Unit III : SECURE COMMUNICATION PROTOCOLS 9

Encryption Principles- Cryptography, Cryptanalysis, Feistel Cipher Structure. Block Encryption algorithms: DES, triple DES, and AES. Transport-Level Security: Secure Sockets Layer (SSL), Transport Layer Security TLS). Electronic Mail Security- Pretty Good Privacy (PGP), S/MIME. Securing wireless networks: WPA, WPA2, WPA3.

Unit IV : INTRUSION DETECTION AND PREVENTION SYSTEMS 9

IDPS- Need of Intrusion Detection Systems in Cyber Security- Types of IDPS: Network-based and Host-based. Configuring and Managing IDPS for threat detection using Honeypots. Case Study: Setup a honey pot and monitor the honey pot on network.

Unit V : WEB APPLICATION SECURITY 9

Introduction to Web Application Vulnerabilities – Cross Site Scripting (XSS) – SQL injection- Denial of Service (DoS)- Web Application Testing - Types of Penetration Tests- OWASP and OWASP Top.

R.M.K GROUP OF INSTITUTIONS

5.COURSE OUTCOME

Course Code	Course Outcome Statement	Cognitive / Affective Level of the Course Outcome	Course Outcome
Course Outcome Statements in Cognitive Domain			
22CS930	Understanding the core concepts and importance of cybersecurity in organizational settings.	Apply K3	CO1
22CS930	Acquire the knowledge common network attacks and deploy appropriate security measures.	Apply K3	CO2
22CS930	Implement encryption and secure communication protocols for data integrity and confidentiality.	Apply K3	CO3
22CS930	Deploy and manage Intrusion Detection and Prevention Systems for threat detection.	Apply K4	CO4
22CS930	Identify and mitigate common web application vulnerabilities	Apply K4	CO5
22CS930	Conduct penetration tests to evaluate the security posture of web applications.	Apply K5	CO6

6.CO-PO/PSO MAPPING

Correlation Matrix of the Course Outcomes to Programme Outcomes and Programme Specific Outcomes.

Course Outcomes (Cos)		Programme Outcomes (POs), Programme Specific Outcomes (PSOs)														
		PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
22CS930.1	K2	3	2	3	-	2	-	-	1	-	-	-	2	3	2	1
22CS930.2	K3	3	3	3	-	3	-	-	-	-	-	-	2	3	3	2
22CS930.3	K3	2	3	3	-	3	-	-	-	1	1	-	2	3	3	2
22CS930.4	K3	2	3	3	-	3	-	-	2	-	-	-	2	3	3	2
22CS930.5	K2	3	2	3	-	2	-	-	-	-	-	-	3	3	3	3
22CS930.6	K3	3	3	3	-	3	-	-	-	-	2	1	3	3	3	3

R.M.K GROUP OF INSTITUTIONS

UNIT I
INTRODUCTION TO CYBERSECURITY

R.M.K GROUP OF INSTITUTIONS

7.LECTURE PLAN – UNIT I

	UNIT I INTRODUCTION						
Sl. No	TOPIC	NO OF PERIODS	PROPOSED LECTURE PEROID	ACTUAL LECTURE PERIOD	PERTAINING CO(s)	TAXONOMY LEVEL	MODE OF DELIVERY
1	Cyber Security – Need of Cybersecurity in Organizations	1			CO1	K2	MD1, MD5
2	CIA Triad-Confidentiality, Integrity, Availability;	2			CO1	K1	MD1, MD5
3	Reason for Cyber Crime-Need for Cyber Security	1			CO1	K2	MD1, MD5
4	History of Cyber Crime; Cybercriminals	1			CO1	K2	MD1, MD5
5	Classification of Cybercrimes– A Global Perspective on Cyber Crimes	2			CO1	K2	MD1, MD5
6	Cyber Laws – The Indian IT Act – Cybercrime and Punishment.	2			CO1	K2	MD1, MD5

R.M.K GROUP OF INSTITUTIONS

LECTURE PLAN – UNIT I

ASSESSMENT COMPONENTS

- AC 1. Unit Test
- AC 2. Assignment
- AC 3. Course Seminar
- AC 4. Course Quiz
- AC 5. Case Study
- AC 6. Record Work
- AC 7. Lab / Mini Project
- AC 8. Lab Model Exam
- AC 9. Project Review

MODE OF DELEIVERY

MD 1. Oral presentation
MD 2. Tutorial
MD 3. Seminar
MD 4 Hands On
MD 5. Videos
MD 6. Field Visit

R.M.K GROUP OF INSTITUTIONS

8. ACTIVITY BASED LEARNING : UNIT – I

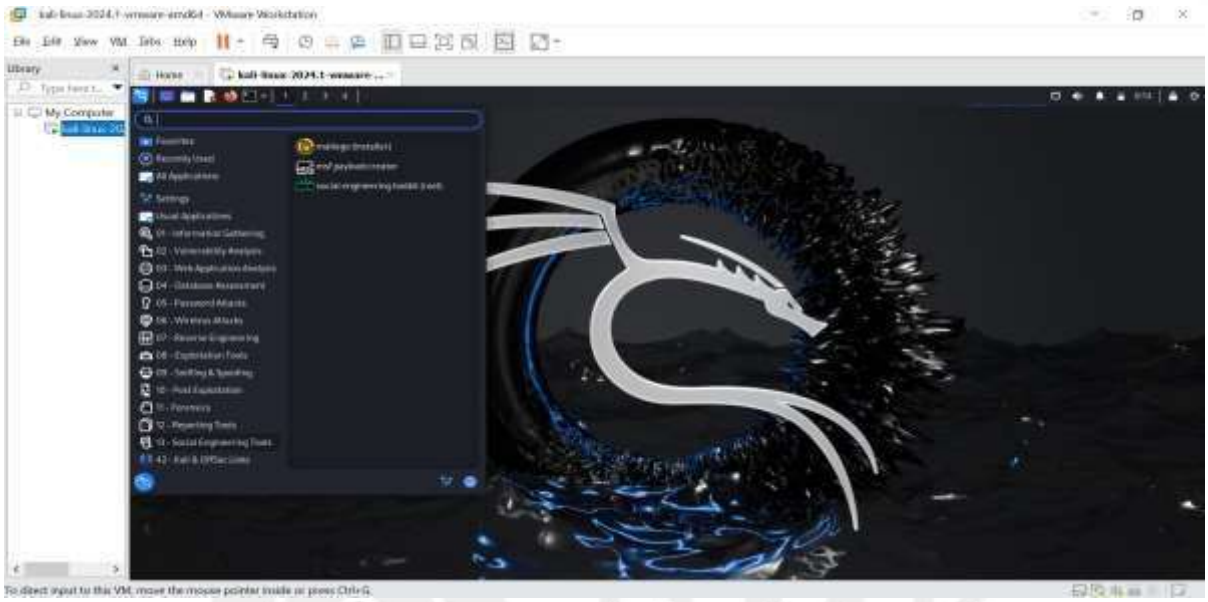
ACTIVITY 1:

Step1: Download and install VMware Workstation Pro

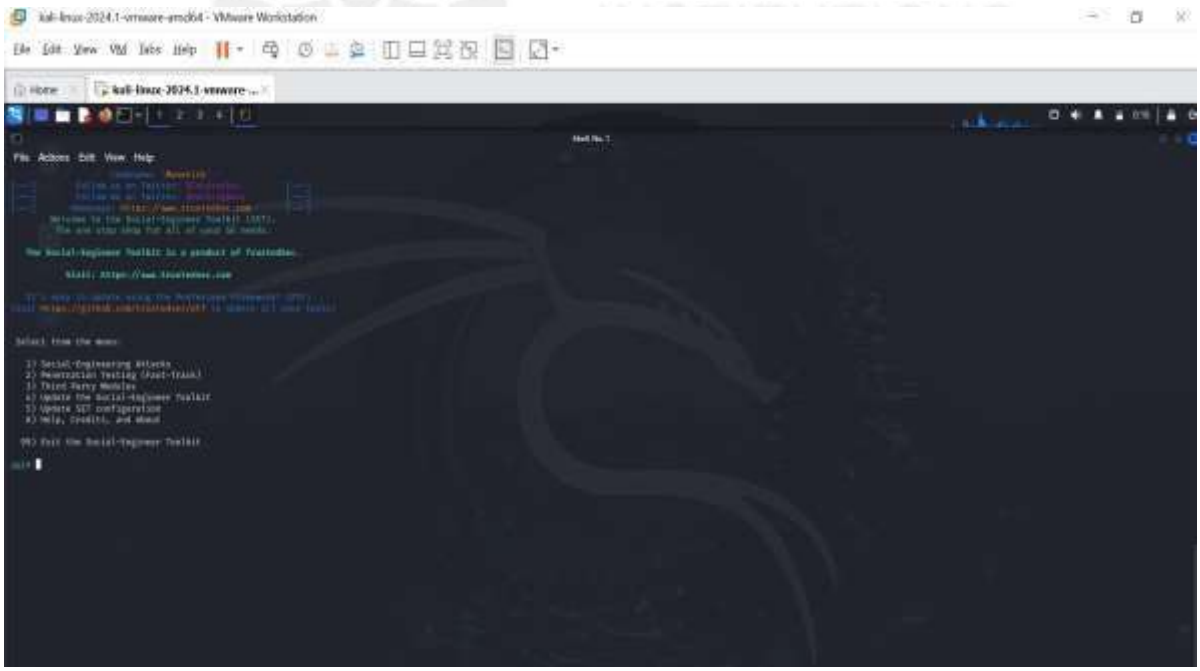
Step2: Download and Install Kali Linux VMware for operating VMware Workstation

R.M.K GROUP OF INSTITUTIONS

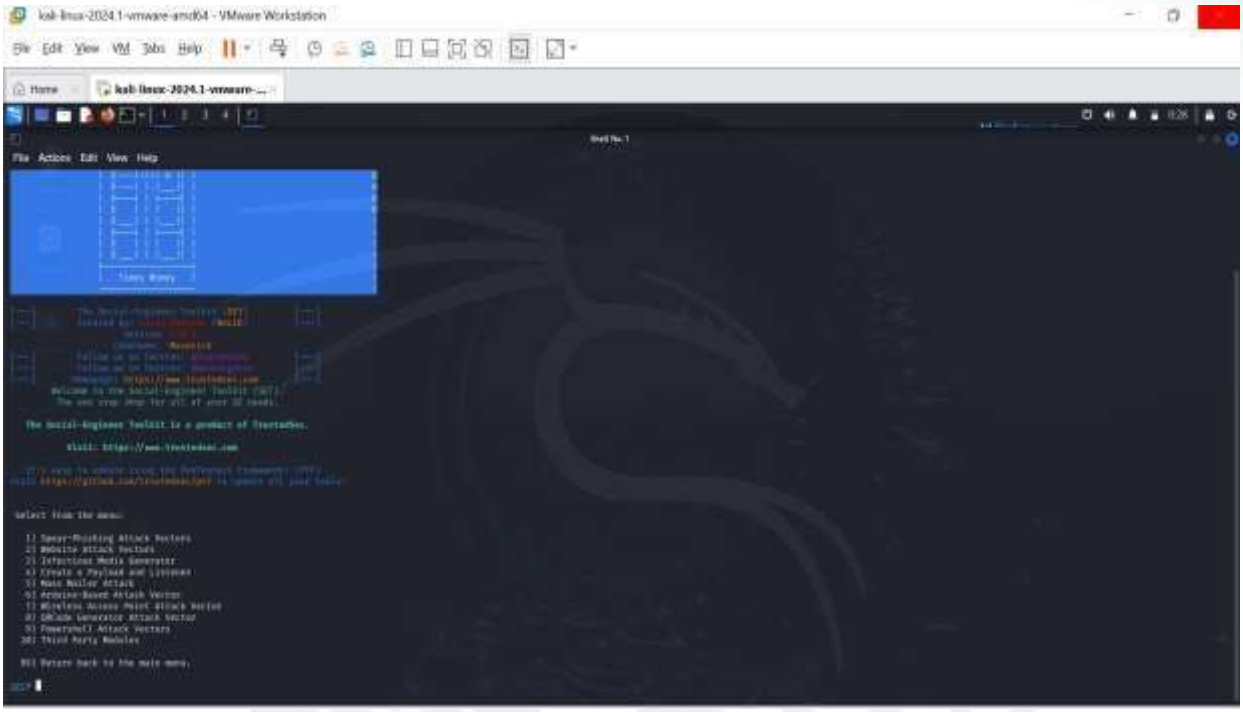
Step3: Select Social Engineering Toolkit application from Social Engineering Tool



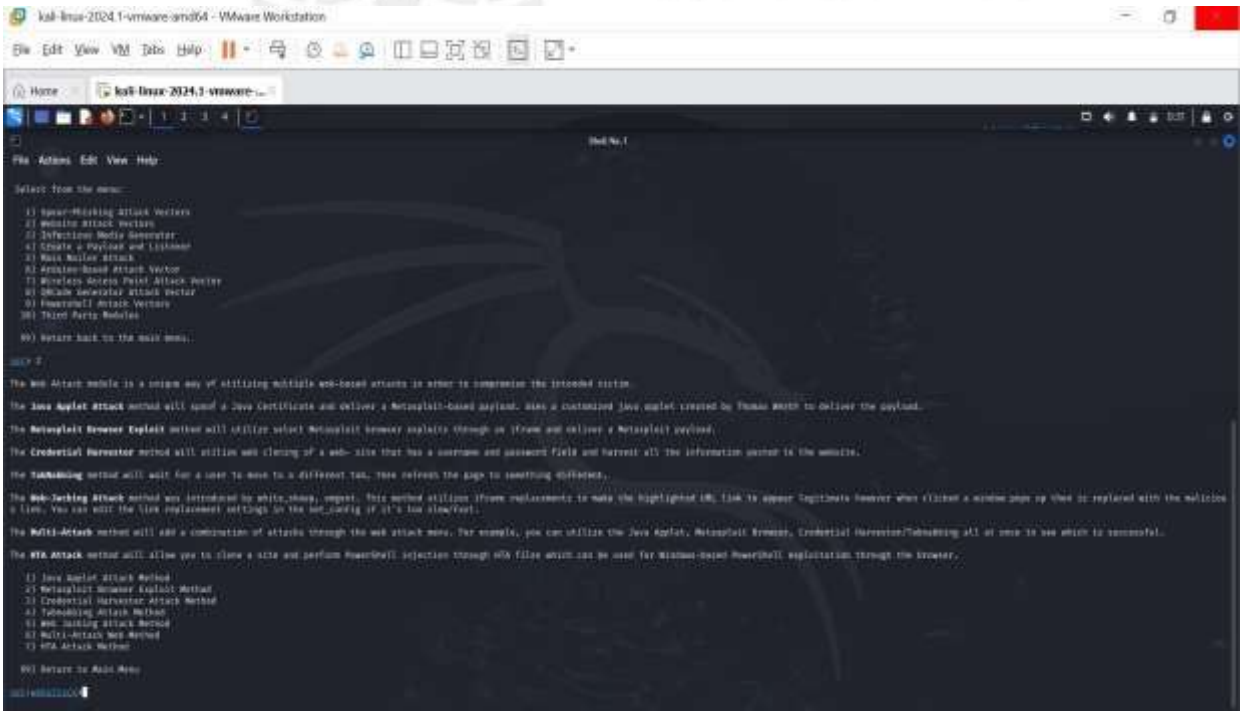
Step 4: Select Social Engineering Attacks from Menu



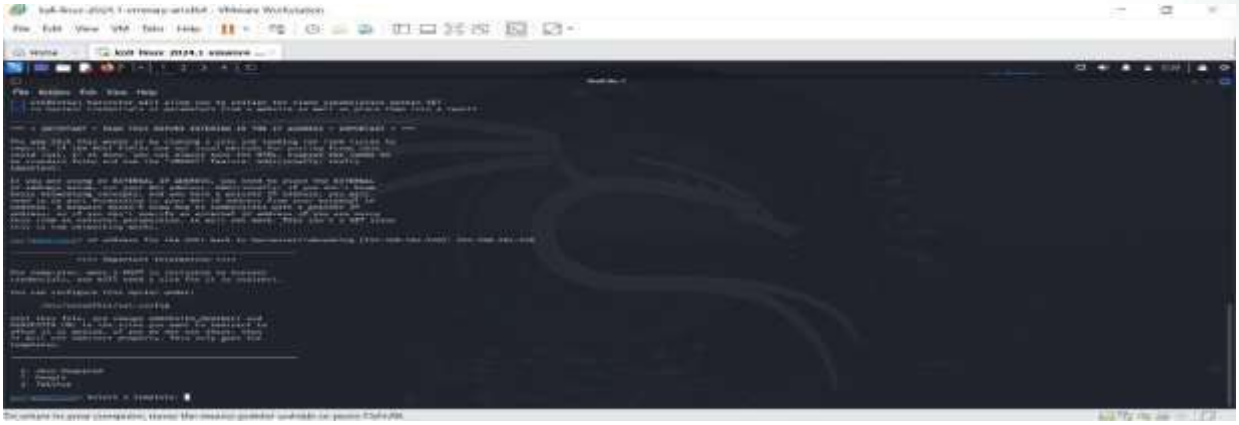
Step 5: Select Website Attack Vectors from Menu



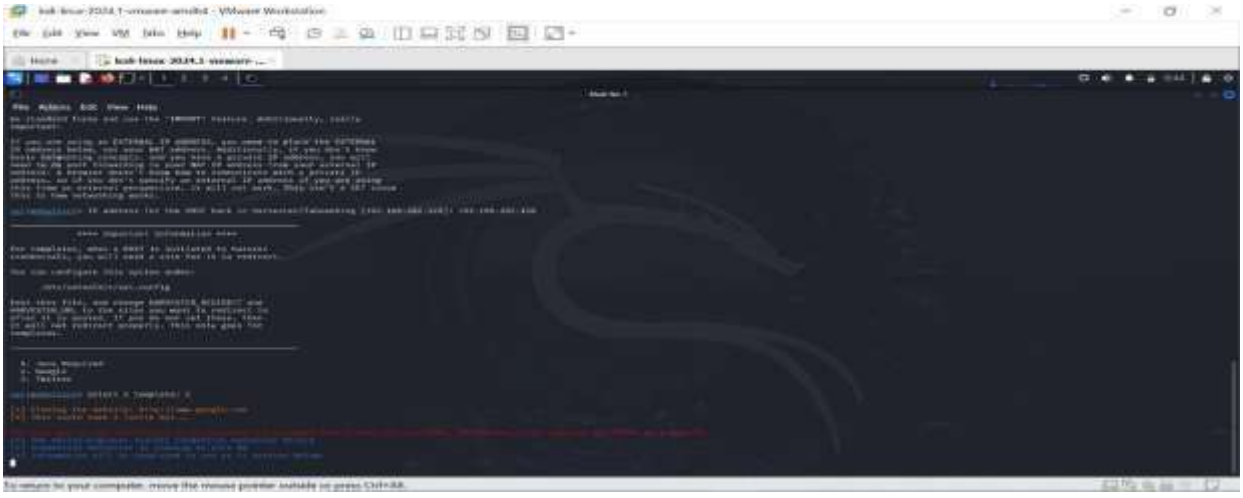
Step 6: Select Credential Harvester Attack Method from Menu



Step 7:Select Template of the website from Menu



Step 8: Connect to the website login page through the IP address and sniff the website credentials



Thus, a social networking website login page is created using phishing techniques.

9. LECTURE NOTES : UNIT – I

INTRODUCTION TO CYBER SECURITY

Syllabus:

Cyber Security – Need of Cybersecurity in Organizations – CIA Triad- Confidentiality, Integrity, Availability; Reason for Cyber Crime –Need for Cyber Security – History of Cyber Crime; Cybercriminals – Classification of Cybercrimes– A Global Perspective on Cyber Crimes; Cyber Laws – The Indian IT Act – Cybercrime and Punishment.

1. INTRODUCTION

What is Cybersecurity?

Cybersecurity refers to the practice of defending computer systems, networks, and data against unauthorized access, cyberattacks, and various digital threats. It encompasses a wide array of strategies, technologies, and procedures aimed at protecting systems and information from malicious activities, data breaches, and other cyber-related risks.

2. Need of Cybersecurityin Organizations

Cybersecurity has become a fundamental requirement for organizations of all sizes, as digital threats grow increasingly sophisticated. It plays a vital role in protecting sensitive data, financial resources, and the overall stability of operations. Here's why it matters:

1. Defense Against Evolving Cyber Threats

Organizations are frequently targeted by cyber threats such as malware, ransomware, phishing, and advanced persistent threats (APTs). Effective cybersecurity measures help prevent unauthorized access and protect systems from being compromised.

2. Protection of Confidential Data

Businesses manage sensitive information, including customer data, financial details, and intellectual property. Without adequate security, this data is at risk of theft or tampering, potentially causing serious financial and reputational harm.

R.M.K GROUP OF INSTITUTIONS

3. Ensuring Business Continuity

Cyberattacks—particularly ransomware—can halt operations and cause extended downtime. Cybersecurity protocols help maintain continuity by reducing the impact of attacks and supporting swift recovery.

4. Regulatory Compliance

Compliance with industry regulations like GDPR, HIPAA, and ISO 27001 requires organizations to maintain strict cybersecurity standards. Failure to comply can result in significant fines and legal repercussions.

5. Strengthening Customer Confidence

Customers expect their personal information to be protected. A strong cybersecurity framework builds trust, reassuring clients that their data is handled securely.

6. Minimizing Financial Risk

Cyber incidents often come with heavy financial consequences—from breach-related costs to legal fees and penalties. Investing in cybersecurity helps mitigate these risks and protect long-term financial health.

7. Mitigating Insider Threats

Threats don't always originate externally. Employees or contractors can unintentionally or deliberately compromise security. Implementing access controls, continuous monitoring, and employee training helps prevent internal breaches.

1.3 CIA TRIAD

The Evolution of the CIA Triad:

CIA Triad is a model designed to guide policies for information security. It provides us with a reference to evaluate and implement secure information systems, independently of the underlying technologies. Each one has specific requirements and processes. CIA Triad is aimed at protecting the organization's digital assets against the ever-growing Cyber-attacks.

The concept of the CIA Triad developed gradually over time, with no single originator:

- Confidentiality was discussed as early as 1976 in a U.S. Air Force study.
- Integrity gained attention in 1987 in a paper comparing commercial and military computer security policies, emphasizing the need for accurate and reliable data.

Figure 1: CIA TRAID

- Availability became more prominent by 1988 and, by 1998, the three concepts were commonly grouped under the term CIA Triad.

Today, the CIA Triad is central to standards such as ISO/IEC 27001:2013, which defines information security as the protection of confidentiality, integrity, and availability of organizational assets.

The CIA Triad helps organizations evaluate and implement information security measures independent of technology platforms. It is especially crucial in protecting digital assets from increasing cyber threats through security features like deterrence, prevention, and detection

Components of the CIA Triad

Figure 2: Confidentiality

1. CONFIDENTIALITY

Confidentiality is closely associated with privacy, aiming to ensure that sensitive data is accessed only by authorized individuals. This principle is vital when data is transmitted over networks or stored in digital formats.

Key Aspects:

Limits data access to only intended and authorized users.

Prevents unauthorized interception and use of data by malicious actors.

Data classification helps determine the appropriate level of confidentiality required.

❖ **Methods to Ensure Confidentiality:**

Encryption: Converts plaintext into unreadable ciphertext using symmetric or asymmetric algorithms.

Authentication mechanisms: Including user IDs, passwords, two-factor authentication, biometrics, and security tokens.

Steganography: Hiding sensitive data within images, audio, or video files.

Access control lists and file permissions: Regularly updated to restrict unauthorized access.

User training: Educates users on password hygiene, social engineering threats, and data-handling best practices.

Real-World Example: Online banking uses token numbers, encryption, and multi-factor authentication to ensure user data remains confidential.

Confidentiality should ensure that

- ❖ Data should be handled based on their required privacy.
- ❖ Data should be encrypted, with a form of two-factor
- ❖ Data should be encrypted, with a form of two-factor authentication to reach it.
- ❖ Keeping access control lists and other file permissions up to date.

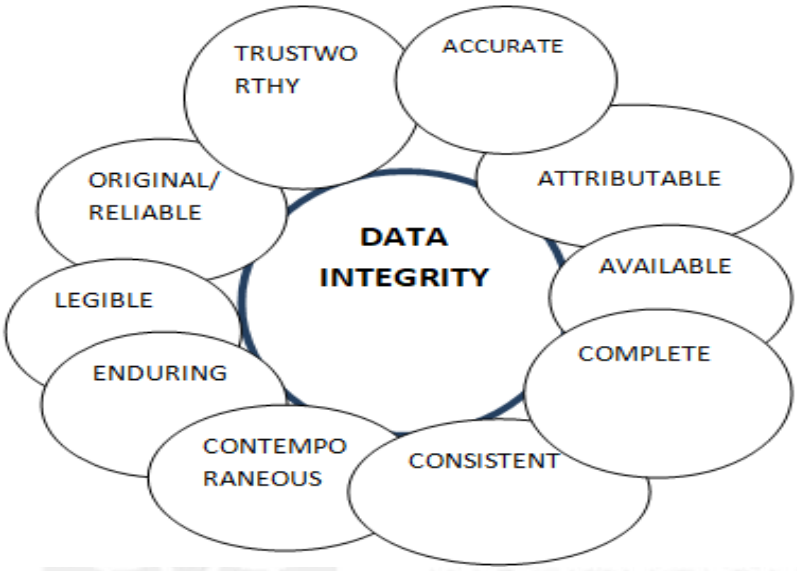


Figure 2: INTEGRITY

1.3.2. INTEGRITY

Integrity involves maintaining the accuracy, consistency, and reliability of data throughout its lifecycle. It ensures that information remains unaltered unless modified by authorized entities.

Core Goals:

Prevent unauthorized modifications to data.

Detect and recover from changes due to cyberattacks or system errors.

Ensure data remains trustworthy and uncorrupted in storage and transit.

❖ **Methods to Ensure Integrity:**

Access and file permission controls.

Version control: Prevents accidental overwrites or deletions.

Cryptographic hashing (e.g., MD5, SHA-1): Used to verify data integrity.

R.M.K GROUP OF INSTITUTIONS

Digital signatures and certificates: Help validate data sources and prevent tampering.

Checksums: Help detect accidental changes.

Backups and redundancies: Allow restoration of accurate data in case of corruption.

Typical Threats:

- ❖ Man-in-the-middle (MITM) attacks
- ❖ Server breaches and injection of malicious code
- ❖ System crashes or non-human-caused disruptions (e.g., EMP)

Integrity should ensure that

1. Employees are knowledgeable about compliance and regulatory requirements.
2. Use a backup and recovery software.
3. To ensure integrity, make use of version control, access control, data logs and checksums.

1.3.3. AVAILABILITY

Availability ensures that authorized users have timely and reliable access to information and systems when needed. It focuses on maintaining system uptime and quick recovery from disruptions.

Figure 3: Availability

Key Requirements:

Continuous operation of systems and services.

Immediate resolution of hardware or software issues.

Mitigation of downtime caused by upgrades or attacks.

R.M.K GROUP OF INSTITUTIONS

Methods to Ensure Availability:

- ❖ Redundant systems and failover mechanisms (e.g., RAID, high-availability clusters).
- ❖ Regular hardware maintenance and prompt repairs.
- ❖ Disaster Recovery Plans (DRPs): Guide quick system recovery in emergencies.
- ❖ Geographically separate data backups (e.g., in fireproof or waterproof safes).
- ❖ Monitoring tools: Track network and server performance to identify bottlenecks.
- ❖ Protection against DoS/DDoS attacks: Firewalls, proxy servers, and rate-limiting tools

Best Practices for Availability:

1. Apply timely system updates and patches.
2. Use real-time monitoring and alert systems.
3. Design robust business continuity and disaster recovery strategies.

Availability

- Use preventative measures such as redundancy, failover and RAID.
- Ensure systems and applications stay updated.
- Use network or server monitoring systems.
- In case of data loss, ensure a Data Recovery and Business Continuity plan is in place.

1.3.4 REASON FOR CYBER CRIME

Committing a crime is one of the most serious offenses a person can commit, as it represents a violation of moral laws and ethical standards. Crimes, including cybercrimes, can be understood through various lenses such as sociological, psychological, environmental, and political perspectives.

One of the first questions often asked during a criminal investigation is, "What was the motive?" With rapid technological advancements, people have become heavily reliant on the internet for nearly every aspect of daily life—social networking, online shopping, digital education, remote jobs, and entertainment.

This growing dependence has also led to the rise of cybercrimes, which have evolved alongside the benefits of the internet. Initially, there was limited awareness about cybercrimes, but with increasing internet usage, such incidents are now on the rise globally, including in countries like India.

Ease of committing these offenses:

One of the key reasons for the surge in cybercrimes is the ease of committing these offenses. Unlike traditional crimes, modern cybercrimes require minimal technical expertise. With the widespread availability of low-cost hacking tools and countless online tutorials on platforms like YouTube and Facebook, even individuals with basic knowledge can learn how to carry out cyber-attacks. Unfortunately, media portrayals often glamorize cybercriminals, influencing impressionable adolescents to emulate such behavior. Moreover, cybercriminals can operate from anywhere in the world, targeting victims globally from the comfort of their homes and launching attacks on multiple locations simultaneously.

High reward-to-risk ratio in cybercrime

Another major contributing factor is the high reward-to-risk ratio in cybercrime. Unlike other forms of crime, cybercrimes pose relatively low physical danger to the perpetrators. Law enforcement and cybersecurity agencies often lag behind technologically, reducing the likelihood of criminals being apprehended. Additionally, the low cost of hacking tools and the accessibility of technical knowledge contrast sharply with the high potential gains. A single successful hack can yield significant financial returns, access to sensitive personal data, and materials that can be used for blackmail or fraud. The combination of low risk and high reward makes cybercrime an increasingly attractive and profitable avenue for criminals.

Anonymity

One of the most significant enablers of cybercrime is the anonymity the internet provides. A growing number of cybercriminals are turning to the encrypted, untraceable parts of the internet—such as the dark web—to purchase software and tools that help them remain undetected while committing illegal activities. The ability to conceal one's identity online makes it incredibly difficult for authorities to trace perpetrators. Traditional methods of tracking, such as tracing an IP address, can easily be bypassed using Virtual Private Networks (VPNs) or techniques like onion routing, which allow for anonymous communication over computer networks. This means that cybercriminals can commit serious offenses, including major cyberattacks, and remain hidden indefinitely.

A striking example is the MyDoom virus, considered one of the most destructive computer viruses in history, which caused over $38 billion in damages. Despite a $250,000 reward offered by Microsoft for information leading to the arrest of its creator, the individual responsible was never identified—highlighting how cybercriminals can often operate without fear of being caught.

Espionage

Cybercrime has evolved into a new frontier for international espionage and warfare. As digital infrastructure becomes a critical national asset—as declared by former U.S. President Barack Obama—nations are increasingly vulnerable to cyber espionage. This form of cybercrime involves unauthorized access to sensitive government or corporate data, often with the intent to damage, disrupt, or gather intelligence.

Cyber espionage is frequently state-sponsored and targets intellectual property, classified documents, and other strategic information. It can support military operations, serve political agendas, or function as a form of cyberterrorism. The consequences can be severe, ranging from reputational damage and stolen personal data to failed military missions and loss of life

A notable case occurred in 2009 when Google detected targeted cyberattacks aimed at Gmail accounts of Chinese human rights activists. Google later discovered that at least 20 other companies were also under attack via a vulnerability in Microsoft Internet Explorer, a campaign later identified by McAfee Labs and dubbed "Aurora."

Another example is the Flame virus, discovered in 2012, which targeted Middle Eastern systems. Unlike Stuxnet, which focused on industrial controls, Flame was a sophisticated general-purpose surveillance virus capable of recording Skype calls, collecting local and network data, and evading antivirus software. These incidents illustrate how cyber espionage can operate silently, collecting vast amounts of sensitive information undetected.

Hacktivism

Hacktivism, a blend of hacking and activism, is the act of breaching digital systems as a form of political or social protest. The term was first coined in 1994 by a member of the hacking group "The Cult of the Dead Cow," which was founded in 1984 in Lubbock, Texas. Hacktivism has gained considerable attention in recent years, as more individuals and groups engage in politically motivated cyber activities. One of the most well-known hacktivist collectives is Anonymous, a loosely organized group formed out of the 4chan online community. Anonymous is known for championing human rights and protesting government surveillance, censorship, and corporate corruption. Their actions include exposing hate groups, targeting child exploitation websites, and retaliating against state-sponsored cyberattacks.

Operations like "Operation Darkness" aimed to combat online child pornography and expose cyber threats from foreign military entities. Hacktivists are not motivated by personal financial gain but by a desire to raise awareness or protest against perceived injustices. Their tactics include leaking sensitive information, defacing websites, or launching denial-of-service (DoS) attacks to disrupt services and draw attention to their causes.

R.M.K GROUP OF INSTITUTIONS

4. NEED FOR CYBERSECURITY

1. IMPACT OF COVID-19 ON CYBERSECURITY AND REMOTE WORK

Sudden Shift to Remote Work

- The COVID-19 pandemic forced organizations to quickly adopt remote working models.
- Most businesses and governments were unprepared for the transition.

Increased Demand on Digital Infrastructure

- Overnight, the need for remote access to office networks surged.
- Employees, many with no prior remote work experience, were asked to connect from home.

Unpreparedness and Struggles

- Many organizations struggled to adapt to the new remote environment.
- Some are still facing challenges in fully adopting remote work securely.

Rise in Cybercrime

- Cybercriminals exploited the crisis for gain, targeting weakened security systems.
- More lucrative and vulnerable targets became accessible outside of organizational perimeter defenses.

Lack of Perimeter Security

- Remote access relied on public internet, which is less secure than internal networks.
- Traditional office-based cybersecurity controls became less effective.

Vulnerability of Existing Systems

- Before the pandemic, secure data access was restricted to office environments.
- Remote work introduced new vulnerabilities in organizations.

New and Unfamiliar Risks

- The shift to digital brought unfamiliar cybersecurity threats.
- Organizations had to address risks they had never faced before.
- Challenges in Enforcing Security Policies
- Managing security for a remote workforce is complex and difficult.
- Security controls often lacked scalability and were time-consuming to deploy.

Use of Personal Devices

- Some businesses allowed employees to use personal devices without proper security measures.
- This increased the risk of unauthorized access and data breaches
- Weak Business Continuity and Incident Response Plans
- Many organizations had outdated or non-existent BCPs and IRPs for a pandemic scenario.
- Few were ready for a large-scale shift to remote operations.
- Necessity of Cybersecurity in the Digital Era
- The digital world is deeply integrated into daily life—banking, shopping, education, etc.
- Lack of cybersecurity is equivalent to having no locks or security systems on a house.

Increased Responsibilities for Security Leaders

- Security professionals must now protect large, remote infrastructures.
- They must ensure resilience against a growing range of cyber threats.
- Urgent Need for Scalable and Secure Remote Access
- Secure access to enterprise systems is now a major challenge.
- Rapid implementation of strong cybersecurity practices is essential for survival and growth.

1.4.2 DAMAGE TO ORGANIZATIONS

In the digital age, data is one of the most valuable assets for any organization—and also the most targeted. As cyber-attacks grow more frequent and sophisticated, many organizations still underestimate their risks, especially when it comes to justifying security budgets. However, the consequences of a successful cyber-attack can be severe and long-lasting, affecting both finances and reputation.

Economic Damage

- Direct Financial Loss: Cyber incidents often involve stolen funds, damaged infrastructure, regulatory fines, and legal settlements.
- Loss of Productivity: Downtime disrupts business operations, leading to immediate financial loss and diverting IT resources from routine work.

Revenue Impact:

- Attacks like DDoS reduce service availability, degrade customer experience, and lead to canceled or postponed orders.
- Response & Recovery Costs: Organizations often need external experts for recovery, adding to costs.

Investigation Expenses:

- Post-incident forensics, auditing, and compliance checks can be complex and expensive.
- Intangible Damage

Loss of Intellectual Property:

- Breached trade secrets, business strategies, and proprietary data can erode competitive advantage and future revenue.

Reputation Loss:

- Customer trust and investor confidence can decline sharply after a breach, affecting future deals and share prices.
- Operational Disruption: Companies without strong continuity plans may struggle to recover, especially smaller businesses facing increased insurance or borrowing costs.

R.M.K GROUP OF INSTITUTIONS

Legal and Regulatory Consequences

- Organizations may face lawsuits from consumers for failing to protect personal data or violating privacy agreements.
- Non-compliance with data protection laws can result in heavy fines and even criminal charges.
- Post-breach PR and legal efforts are necessary to manage public image and communicate with stakeholders and regulators.

1.5 HISTORY OF CYBERCRIME

Digital technology has revolutionized connectivity, offering numerous benefits—but it has also created a fertile ground for cybercrime. From vandalism and identity theft to the breach of classified information, the digital landscape has enabled a range of criminal activities, commonly referred to as hacking. Cybercrime has become one of the most profitable crimes in the modern era—easy to commit, rewarding, and with a low perceived risk of punishment. As a result, its growth has been exponential.

A Brief History of Cyber-Crime

Interestingly, cybercrime began even before the invention of computers. Some major milestones include:

- 1834: The first recorded cyber-attack occurs when two Frenchmen hack the telegraph system to steal financial data.
- 1870s–1900s: Early telephone systems were exploited by teenagers to reroute and misuse calls.
- 1903: Nevil Maskelyne disrupted a secure wireless communication demo using Morse code.
- 1939: During WWII, Alan Turing helped break the Enigma code with the electromechanical device "Bombe."
- 1955: A whistle mimicking phone tones allowed free long-distance calls—an early example of exploiting telecommunications.

The Computer Age and Rise of Phreakers

- 1962: MIT created one of the first password systems. Student Allan Scherr bypassed restrictions using stolen credentials.
- 1969: A self-replicating program overloaded systems at the University of Washington—a precursor to modern viruses.
- 1970s: "Phreakers" exploited phone systems using tone generators. John Draper (aka "Captain Crunch") led the way, inspiring Steve Jobs and Steve Wozniak.

The Evolution of Cyber-Crimes (1970s–2000s)

Cybercrime advanced with the development of computers and the internet. Key events include:

- 1971: Draper builds a device to make free calls. This marked the beginning of wire fraud via telecom exploitation.
- 1973: A bank employee embezzled $2 million using a computer.
- 1978: The first Bulletin Board System (BBS) launches, facilitating hacker communication.
- 1981: Ian Murphy (Captain Zap) becomes the first convicted hacker after altering AT&T's billing system.
- 1982: A 15-year-old writes "Elk Cloner," an early virus that spreads via floppy disk.
- 1983: WarGames movie brings hacking into pop culture.
- 1986: The U.S. enacts the Computer Fraud and Abuse Act.
- 1988: The Morris Worm infects 600,000 systems on ARPANET, the precursor to the Internet.
- 1989: The first case of ransomware emerges via the "AIDS Trojan," demanding $500 for data recovery.
- 1990s: Cyber gangs like the Legion of Doom and Masters of Deception dominate the underground, triggering FBI crackdowns.

The Modern Cybercrime Era (1994–2003)

- 1994: With the launch of the World Wide Web, hackers shift from BBS forums to personal websites.
- 1995: Macro-viruses emerge, embedded in Word and Excel documents.

R.M.K GROUP OF INSTITUTIONS

- 1996–1997: Reports surface of massive breaches in U.S. government and corporate networks. 85% of U.S. firms were reportedly hacked.
- 1999: The Melissa Virus, a macro-virus, infects email systems and causes over $80 million in damages.
- 2000: A wave of high-profile cyber-attacks begins—CD Universe is extorted, DDoS attacks hit major companies, and the "ILOVEYOU" virus causes global disruption.
- 2002: ShadowCrew, a hacker forum, is shut down after international arrests.
- 2003: SQL Slammer, a rapidly spreading worm, affects 75,000 machines in under 10 minutes, severely impacting internet performance.

PROMINENT CYBER SECURITY BREACHES:

Compromised Company	Records Exposed	Discovered
Quest Diagnostics	11.9 million	2018–2019
Marriott	500 million	2014–2018
Equifax 2017	145.5 million	2017
Facebook	50 million	2017
Yahoo	3 Billion	2013
Linkedin	100 million	2012
Uber	57 million	2016

1.6 CLASSIFICATION OF CYBER-CRIME

Cyber-crimes, like traditional crimes, can be grouped based on shared characteristics. One widely accepted approach classifies cyber-crimes into two broad categories: active and passive.

❑ **Active Cyber-Crimes** involve direct use of a computer to commit a crime—for example, unauthorized access to a secured network (hacking).

❑ **Passive Cyber-Crimes** involve using a computer to support illegal activities, such as tracking drug transactions or managing illicit profits.

Classification by Role of the Computer in the Crime

Computer as the Target

These crimes directly attack computer systems, networks, or data. Examples include:

✓ Hacking into restricted networks

✓ Spreading malware or viruses

✓ Data theft (personal, financial, or classified information)

Computer as a Tool (Instrumentality)

In this category, computers are used to commit traditional crimes more efficiently. Examples include:

✓ ATM fraud

✓ Credit card scams

✓ Financial fraud via online transactions or telecom systems

Computer as an Incidental Component

Here, the computer isn't central to the crime but is used to facilitate it. Examples:

✓ Money laundering

✓ Illegal banking transactions

✓ Managing organized crime records or bookkeeping for illegal operations

R.M.K GROUP OF INSTITUTIONS

Crimes Stemming from the Widespread Use of Computers

These crimes have emerged due to the proliferation of digital technology.

Examples include:

- ✓ Software piracy and copyright infringement
- ✓ Distribution of counterfeit software or hardware
- ✓ Theft and resale of computer technology or equipment

Classification by Target of the Attack

Crimes Against Individuals

These crimes directly impact a person's privacy, reputation, or property. Examples:

- ✓ Email harassment and cyberstalking
- ✓ Distribution of obscene or offensive content
- ✓ Financial fraud, including unauthorized transfers or credit card misuse

Crimes Against Organizations or Nations

These are often politically or ideologically motivated and target institutions.

Examples:

- ✓ Defacing or shutting down military or government websites
- ✓ Spreading disinformation or propaganda through digital platforms

TYPES OF CYBER CRIMES

Phishing is a type of cyber-attack where attackers deceive individuals into taking harmful actions that can compromise their security. It is commonly used to gather personal information through misleading emails, social media posts, or websites. In these attacks, emails are disguised to appear trustworthy and persuasive. The aim is to fool the recipient into thinking the message is something important or desirable—such as a communication from a bank, a familiar individual, a government agency, or even a colleague—prompting them to click a link, download an attachment, or share sensitive information like banking credentials or personal data.

R.M.K GROUP OF INSTITUTIONS

Cybercriminals often pose as credible entities, such as real companies or individuals the victim might know or trust. Phishing is one of the oldest forms of cyber-attacks, originating in the 1990s, and continues to be one of the most prevalent and dangerous due to its evolving sophistication. The term "phish" is pronounced like the word "fish," drawing an analogy to casting a baited hook into cyberspace and hoping someone bites. The spelling with "ph" is a nod to hacker slang, likely influenced by "phreaking"—a form of phone hacking involving sound tones to make free calls.

One of the earliest notable phishing incidents occurred in the mid-1990s, when hackers targeted AOL users. In 2004, the first legal action for phishing was taken against a teenager from California who created a fake version of the America Online (AOL) website. By doing so, he managed to collect sensitive user data and accessed credit card information to withdraw funds fraudulently.

Common features of phishing attacks include:

Too Good To Be True: Phishing messages often promise extravagant rewards or prizes to grab attention—like winning a lottery or receiving a free smartphone. If an offer sounds too good to be true, it likely is.

Sense of Urgency: Cybercriminals frequently create urgency by pressuring users to act quickly, claiming that special deals are available only for a limited time. In some cases, they may warn that the user's account will be suspended unless they provide updated personal information immediately. Legitimate organizations typically allow sufficient time for account-related actions and do not request sensitive details through such channels.

•**Hyperlinks:** The displayed link may not match the actual destination. Hovering over a hyperlink reveals the real URL, which may be completely different or a deceptively similar address—for example, "www.Amazon.com" might be altered to something like "www.Amazun.com," where the letter 'o' is replaced with a 'u'.'

•**Attachments:** Phishing emails often include attachments intended to trick recipients into downloading malware such as ransomware or viruses. If an attachment is unexpected or seems out of place, it's best not to open it. The safest type of file to open is a simple .txt file.

•**Unusual Sender:** These emails or messages might appear to come from someone familiar or might impersonate a trusted source. They often mimic the tone and layout of legitimate communication to gain trust.

Phishing attacks can even take the form of messages from unknown or seemingly known contacts. These messages might appear normal but are actually out of character or suspicious. The attacker may pretend to be someone the victim knows to build trust.

Phishing Statistics:

✓ Nearly one-third of all data breaches in 2019 were linked to phishing.

✓ One in every 25 branded emails was a phishing attempt, with the most impersonated brands being Microsoft (42%) and Amazon (38%).

✓ In 2019, 76% of organizations worldwide reported being targeted by phishing.

✓ In 2012, 91% of cyber-attacks began with a spear-phishing email.

✓ URL phishing detections rose by 269% in 2018.

Cyber Bullying

Cyber-bullying is defined as bullying that occurs through the use of digital technology. It can happen via devices such as mobile phones, computers, and tablets. The bullying may occur through SMS, texts, apps, social media platforms, online gaming environments, or anywhere digital content can be shared or interacted with.

Forms of Cyber Bullying:

- Exclusion: Intentionally leaving someone out of online conversations, activities, or social media interactions. Victims may be excluded due to not having the latest devices or access to certain platforms.

- **Harassment:** Persistent and deliberate bullying involving abusive or threatening messages sent to an individual or group. This can severely damage the victim's mental health.

- **Outing:** Posting private or embarrassing personal information about someone online without their consent, often to cause public humiliation.

- **Cyber Stalking:** Involves harassing victims through online communications like emails or social media. It can also include adults targeting young individuals for abusive reasons via the Internet.

- **Fraping:** A term combining "Facebook" and "rape," it refers to unauthorized use of someone's Facebook or other social media accounts to post inappropriate content, impersonating the victim. These posts may remain on the internet even after being deleted.

- **Fake Profiles:** Attackers create fake identities or use someone else's email or phone number to harass a victim anonymously.

- **Dissing:** Posting or sending cruel or hurtful messages aimed at damaging someone's reputation or relationships. This includes sharing harmful photos, screenshots, or videos.

- **Trickery:** Gaining a victim's trust to obtain private information, which is later shared publicly to embarrass or shame the person.

R.M.K GROUP OF INSTITUTIONS

- **Trolling:** Deliberately posting inflammatory or offensive messages on social platforms or forums to provoke a response. Trolls often target individuals to elicit anger or frustration.

- **Catfishing:** Stealing someone's online identity or creating a fake persona by copying profile information. The aim is deception, often leading to reputational harm for the victim.

Common Platforms Where Cyber Bullying Occurs:

✓ Text messaging and messaging apps on mobile phones, tablets, or similar devices
✓ Instant messaging, direct messaging, and online chats
✓ Online forums, chat rooms, and message boards like Reddit
✓ Social media platforms including Facebook, Instagram, Snapchat, and TikTok
✓ Email
✓ Online gaming communities

Identity Theft

Identity theft, also known as identity fraud, refers to the unauthorized use of an individual's personally identifiable information by another person—often a stranger—without the individual's consent or awareness. This form of impersonation is typically carried out to commit fraud, resulting in financial loss for the victim and gain for the perpetrator.

In this context, "identity" refers to both public and private information unique to a specific individual. This includes publicly available details like telephone numbers and home addresses, as well as sensitive information such as Aadhaar numbers, credit card details, and a mother's maiden name. When cybercriminals gain access to such information, they can impersonate the individual and engage in fraudulent online activities.

Although identity theft is most commonly associated with financial fraud, it is also used to gain unauthorized access to services, benefits, or privileges. In some cases, it is even used as a tool for cyberbullying. The stolen identity information can be used to rack up debts, purchase goods or services, or create fake credentials in the victim's name.

One of the most troubling aspects of identity theft is that its consequences may not be immediately apparent. It often takes months—or even years—for victims to realize their information has been misused. Unfortunately, identity theft is becoming increasingly common as cybercriminals adopt more advanced techniques.

Cyber attackers are now exploiting weakly protected social media accounts as a starting point to access more critical areas of a person's digital and financial life. In 2019 alone, 14.4 million consumers fell victim to identity fraud—approximately 1 in every 15 people.

Additional statistics highlight the widespread nature of this crime:
33% of U.S. adults have experienced identity theft, which is over twice the global average. A new victim of identity theft emerges every 2 seconds. In many cases, the victim is not at fault—about one-third of identity theft incidents occur due to factors beyond the individual's control.

- ✓ In 2017, there were 1,579 data breaches, exposing 179 million personal records.
- ✓ One in five identity theft victims has been targeted more than once.
- ✓ In 2017, over 1 million children in the U.S. became victims of identity theft, costing their families a total of $540 million in out-of-pocket expenses.

Identity theft is the most common outcome of a data breach, occurring in 65% of such incidents.Criminals often obtain this personal data through various deceptive and malicious methods, including:

- Posting fake job advertisements to collect resumes and application forms, which typically include names, addresses, email IDs, phone numbers, and sometimes even banking information.
- Phishing attacks, where victims are tricked into revealing personal data via fraudulent emails or websites.
- Exploiting browser vulnerabilities or using malware such as Trojan horse programs and keystroke loggers to capture sensitive information.
- Hacking into computer networks, systems, and databases, allowing attackers to retrieve massive amounts of personal data in a single breach.

As technology evolves, identity theft remains a serious and growing cyber threat, making data protection and user awareness more critical than ever.

Cyberstalking is a criminal act in which an attacker harasses a victim using electronic communication tools such as email, instant messaging (IM), online forums, and discussion groups. The cyberstalker often relies on the anonymity provided by the internet to conceal their true identity. They target victims by sending threatening or abusive messages and may track their online activities.

Cyberstalking can take several forms, depending on the tactics used and the intent of the stalker. Below are common forms of cyberstalking:

1. **Harassment via Email or Messaging**

✓ Sending repeated, unwanted, and threatening emails or messages.

✓ Bombarding the victim with excessive or disturbing communication.

2. Social Media Stalking

✓ Monitoring and commenting obsessively on a victim's posts or activities.

✓ Creating fake profiles to follow or harass the victim.

✓ Sharing private content without consent.

3. Impersonation

✓ Creating fake accounts pretending to be the victim.

✓ Posting false or harmful information under the victim's name.

✓ Using impersonation to damage the victim's reputation or relationships.

R.M.K GROUP OF INSTITUTIONS

4. Cyberbullying

✓ Publicly shaming, mocking, or threatening the victim online.

✓ Spreading rumors or lies on social media, forums, or websites.

✓ Inviting others to join in the harassment.

5. Surveillance and Monitoring

✓ Using spyware, stalkerware, or hacked devices to track the victim's online activity.

✓ Monitoring location through GPS or social check-ins.

6. Doxxing (Publishing Private Information)

✓ Releasing the victim's personal details (address, phone number, workplace, etc.) online.

✓ Encouraging others to harass or harm the victim based on this information.

7. Geotags are pieces of metadata attached to photos, videos, or social media posts that include geographic location information (like GPS coordinates). While often used to share where a photo was taken or where someone checked in, geotags can also be misused by cyberstalkers to track a victim's location.

Hacking is the act of gaining unauthorized access to computer systems, networks, or data. It can be done for various reasons — from malicious intent (such as stealing data or causing harm) to ethical purposes (such as exposing vulnerabilities to improve security).

Types of Hacking:

Black Hat Hacking (Malicious Hacking):

Illegal and harmful.

Involves stealing data, spreading malware, damaging systems, or causing disruption.

Example: Hacking into a company's database to steal customer credit card details.

R.M.K GROUP OF INSTITUTIONS

White Hat Hacking (Ethical Hacking):

✓ Legal and authorized.

✓ Performed by cybersecurity experts to test and strengthen security systems.

Example: Penetration testers hired by companies to find vulnerabilities.

Grey Hat Hacking:

✓ Falls between black hat and white hat.

✓ Hacker may access systems without permission but without malicious intent (e.g., to expose flaws and demand a reward).

✓ Still often considered illegal.

Hacktivism:

✓ Hacking done for political or social causes.

✓ Involves defacing websites, leaking sensitive documents, or disrupting services as protest.

Script Kiddies:

✓ Inexperienced hackers who use existing tools or scripts to launch attacks without fully understanding how they work.

✓ Typically less sophisticated but still capable of causing damage.

Common Hacking Methods:

Phishing: Tricking users into revealing personal information via fake emails or websites.

Malware: Installing malicious software to damage systems or steal data.

Brute Force Attacks: Attempting all possible password combinations to break into accounts.

Keylogging: Capturing everything typed on a victim's keyboard.

SQL Injection: Exploiting flaws in web applications to access or manipulate databases.

R.M.K GROUP OF INSTITUTIONS

Man-in-the-Middle (MitM) Attacks: Intercepting communication between two parties without their knowledge.

Ransomware: Encrypting a victim's files and demanding payment for their release.

Logic Bombs: Definition and Explanation

A logic bomb is a piece of malicious code intentionally inserted into a software system that triggers a harmful function only when certain conditions are met. Unlike viruses or worms, logic bombs remain dormant until activated by specific actions or events.

Key Characteristics of Logic Bombs:

Dormant Until Triggered: The code lies hidden and inactive until a specific trigger occurs (e.g., a particular date, file opened, or user action).

Designed for Harm: Once triggered, it can delete files, corrupt data, disable systems, or open backdoors for attackers.

Often Insider-Planted: Logic bombs are frequently inserted by disgruntled employees, contractors, or others with access to the system.

Common Triggers:

- ✓ A specific date or time (e.g., April 1st).
- ✓ A user logging in or opening a particular application.
- ✓ A certain number of files being deleted or modified.
- ✓ A specific condition in the system not being met (e.g., an employee being removed from payroll).

How to Protect Against Logic Bombs:

Code Audits: Regularly review source code and scripts for unauthorized or suspicious logic.

R.M.K GROUP OF INSTITUTIONS

An Application Layer DDoS attack targets the top layer (Layer 7) of the OSI model — the layer where websites and web applications interact with users. These attacks aim to overwhelm specific functions or features of a website or app, such as login pages, search fields, or shopping carts.

Mimics Legitimate Traffic: Hard to detect because it looks like real user behavior.
Low Bandwidth, High Impact: Doesn't require massive traffic like volumetric attacks but still cripples functionality.

Targets Specific Application Functions: Especially those that require significant server processing (e.g., database queries).

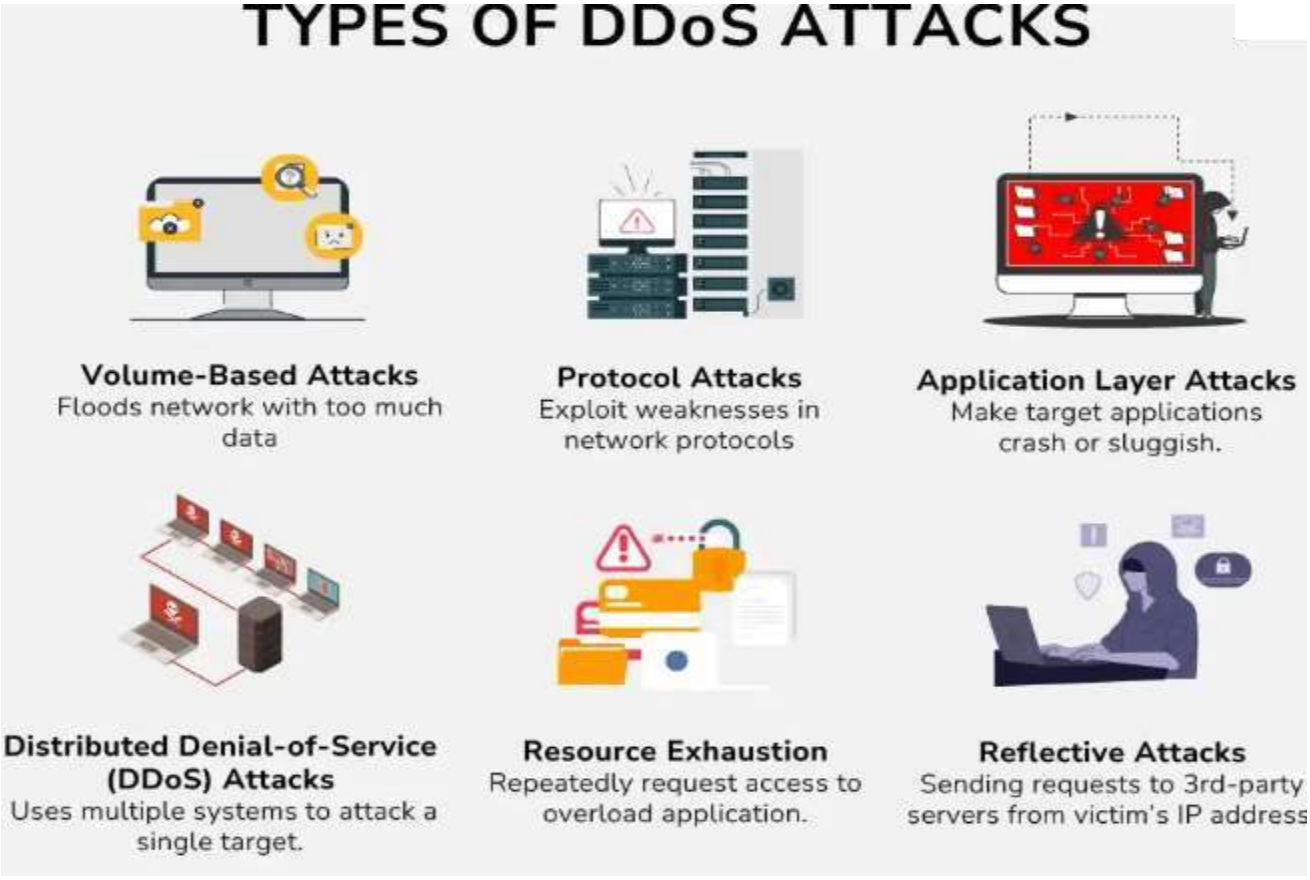


Figure 4: DDoS Attack

Type Description

HTTP GET/POST Flood Sends a high volume of requests for web pages or form submissions. Overloads web servers and backends.

Slowloris Attack Opens many HTTP connections and keeps them alive by sending partial requests slowly. Ties up server resources, causing timeouts.

DNS Query Flood Sends a flood of seemingly legitimate DNS requests. Disrupts domain name resolution, affecting access.

Login Page Attacks Bombards login forms with credentials (brute force or junk data). Drains database and authentication system resources.

Search Function Abuse Repeatedly triggers search or filter functions on a website. Forces server-side processing, causing slowdowns.

Slow Read Attack

A Slow Read Attack is a type of application layer DDoS (Denial-of-Service) attack where the attacker exploits the way web servers handle data transmission, particularly how they send data to clients over TCP connections. This attack does not rely on high traffic volume but instead leverages slow, deliberate data reads to tie up server resources.

How a Slow Read Attack Works

In a normal client-server interaction, a server sends data to a client, and the client acknowledges receiving it and reads it at a reasonable speed. In a Slow Read Attack: The attacker sends legitimate HTTP requests to the server.

However, the attacker's client reads the server's response very slowly by advertising a very small TCP receive window size (the buffer size that determines how much data the server can send at once).

The server continues to keep the connection open, waiting for the client to read the data.

R.M.K GROUP OF INSTITUTIONS

The attacker opens many such slow connections simultaneously, exhausting the server's connection pool and preventing it from serving legitimate users.

A **Large Payload POST Attack** is a type of application-layer DDoS attack that targets a web server's HTTP POST handling mechanism by sending very large payloads in HTTP POST requests. The intent is to consume the server's processing power, memory, and bandwidth, leading to resource exhaustion and service disruption.

How a Large Payload POST Attack Works

The attacker sends numerous HTTP POST requests to the server, each with a massive payload (i.e., a large body of data). These payloads can be gigabytes in size, especially when targeting upload forms, APIs, or file submission portals.

The server allocates memory and processing resources to handle and store each incoming request before validating its content. When repeated many times across multiple connections (especially using botnets), the server becomes overloaded, unable to process requests from legitimate users.

Types of Network Layer DDoS Attacks

Network Layer DDoS attacks target layers 3 and 4 of the OSI model—the network and transport layers—aiming to overwhelm the target's infrastructure (such as routers, firewalls, and servers) with massive volumes of traffic. These attacks are typically high-volume, fast-acting, and designed to saturate bandwidth or exhaust network resources, resulting in denial of service.

Common Types of Network Layer DDoS Attacks

1. UDP Flood

- ✓ Description: Sends a large number of User Datagram Protocol (UDP) packets to random ports on a target system.
- ✓ Impact: The target tries to process each packet and reply with ICMP "Destination Unreachable" messages, consuming resources.
- ✓ Characteristics: Connectionless, hard to trace, often spoofed.

2. ICMP Flood (Ping Flood)

- ✓ Description: Overwhelms the target with a flood of ICMP Echo Request (ping) packets.
- ✓ Impact: The server uses resources to reply to each ping, resulting in system slowdown or failure.
- ✓ Characteristics: Simple to execute but effective on poorly protected systems.

3. SYN Flood

- ✓ Description: Exploits the TCP handshake process by sending numerous SYN requests without completing the connection.
- ✓ Impact: The server allocates memory for half-open connections, which never complete, exhausting available resources.
- ✓ Characteristics: Disrupts connection availability for legitimate users.

4. TCP Connection Flood

- ✓ Description: Initiates many full TCP connections to overwhelm the server's connection table.
- ✓ Impact: Server becomes unable to accept new, legitimate connections.
- ✓ Characteristics: Harder to detect than SYN flood because connections seem legitimate.

R.M.K GROUP OF INSTITUTIONS

5. TCP Reset Attack

- ✓ Description: Sends forged TCP RST (reset) packets to a server or client in an active session.
- ✓ Impact: Abruptly terminates legitimate TCP connections, disrupting communications.
- ✓ Characteristics: Requires knowledge of TCP session details (e.g., sequence numbers).

6. IP Fragmentation Attack

- ✓ Description: Sends fragmented IP packets that overwhelm the target's packet reassembly buffers.
- ✓ Impact: The server must reassemble excessive or malformed fragments, consuming memory and processing power.
- ✓ Examples: Teardrop attack, Overlapping Fragment attack.
- ✓ Characteristics: Exploits how IP fragmentation is handled by the system.

7. Smurf Attack

- ✓ Description: Sends ICMP requests with the spoofed source IP address of the victim to a network broadcast address.
- ✓ Impact: All devices on the network respond to the victim, causing an amplification of traffic.
- ✓ Characteristics: Can generate massive traffic with relatively low input.

8. Ping of Death

- ✓ Description: Sends malformed or oversized ping packets that exceed the maximum size allowed by the protocol.
- ✓ Impact: Older systems may crash or reboot upon receiving such packets.
- ✓ Characteristics: Mostly obsolete, but still affects outdated systems.

R.M.K GROUP OF INSTITUTIONS

Salami attack

A salami attack is a method of cybercrime that attackers or a hacker typically used to commit financial crimes. Cybercriminals steal money or resources from financial accounts on a system one at a time. This attack occurs when several minor attacks combine to create a sturdy attack. because of this sort of cybercrime, these attacks frequently go undetected. Salami attacks are used for the commission of economic crimes Those who are found guilty of such an attack face punishment under Section 66 of the IT Act.

Email Bombing

Email Bombing is a type of cyberattack where a large volume of emails is sent to a single email address in a very short span of time. The goal is to overwhelm the inbox, causing it to crash or become unusable, thereby disrupting communication and potentially hiding more malicious activities like password resets or account takeovers.

Types of Email Bombing:

- ✓ Mass Email Bombing: Sending thousands of duplicate messages.
- ✓ List Bombing: Signing the victim up to numerous mailing lists or newsletters.
- ✓ Zip Bombing: Sending compressed files that expand into large volumes of data, overwhelming the system if opened.

Impact:

- ❖ Crashes email servers or inboxes.
- ❖ Disrupts business communications.
- ❖ May act as a smokescreen to hide other malicious activities.
- ❖ Prevention Measures:
- ❖ Use of spam filters and rate-limiting on incoming emails.
- ❖ Monitoring email traffic for unusual spikes.
- ❖ Blocking known spam IP addresses.

R.M.K GROUP OF INSTITUTIONS

1.7 A Global Perspective on Cyber Crimes;

Cybercrime, a global issue, involves criminal activities using computers and the internet, encompassing various acts like hacking, data theft, and fraud. The Indian Information Technology Act, 2000, forms the primary legal framework for addressing cybercrime in India, defining various offenses and prescribing punishments. Globally, efforts are underway to create comprehensive cybercrime conventions, but challenges remain in dealing with the borderless nature of cybercrime and the rapid evolution of technology.

Global Perspective on Cybercrime:

Borderless Nature:

Cybercrime is not limited by geographical boundaries, making it a global issue.

Rapid Technological Changes:

The ever-evolving nature of technology presents challenges in effectively prosecuting cybercriminals.

International Cooperation:

Efforts to address cybercrime require international cooperation and the development of uniform laws.

Examples:

Cyberattacks can range from large-scale security breaches to targeted harassment of individuals.

UN Initiative:

The UN has been actively working on developing a comprehensive international convention on cybercrime.

Council of Europe:

The Council of Europe has also been working on international treaties and legal frameworks to address cybercrime.

1.8 Cyber Laws:

An Overview Cyber laws are legal frameworks that deal with crimes, frauds, and disputes related to electronic devices, networks, and data.

Importance in Enterprise Cybersecurity:

✓ Protects enterprise data from unauthorized access and breaches.

✓ Sets legal accountability for actions in cyberspace.

✓ Ensures secure online business transactions.

1.9 Indian IT Act, 2000:

India's primary legal framework for dealing with cybercrime is the Information Technology (IT) Act, 2000, which was amended in 2008 to address emerging threats.

Objectives of the IT Act:

✓ Grant legal recognition to electronic documents.

✓ Facilitate electronic filing of documents with government agencies.

✓ Prevent cybercrime and prescribe penalties for such activities.

1.10 Cybercrime & Punishments:

Cybercrime refers to criminal activities that involve a computer, network, or digital device.

Common Types Affecting Enterprises:

✓ Phishing & Social Engineering

✓ Ransomware

✓ AttacksData

✓ Breaches

✓ DDoS Attacks (Distributed Denial of Service)

✓ Insider Threats

✓ Malware and Spyware Injections

R.M.K GROUP OF INSTITUTIONS

Punishment and Legal Consequences:

Cybercrimes under the IT Act are punishable by:

- ✓ Fines: Up to ₹1 crore for damage to systems.
- ✓ Imprisonment: Varies from 3 to 10 years depending on the severity.
- ✓ Compensation: Enterprises can seek damages for data theft or service disruption.

Section	Offense	Punishment
43	Unauthorized access to systems	Compensation to affected parties
66	Hacking and data theft	Up to 3 years imprisonment and ₹5 lakh fine
66C	Identity theft	Up to 3 years imprisonment and ₹1 lakh fine
66D	Cheating by impersonation (online fraud)	Up to 3 years imprisonment and ₹1 lakh fine
66E	Violation of privacy (unauthorized image capture)	Up to 3 years imprisonment and ₹2 lakh fine
67	Publishing obscene material	3-5 years imprisonment and up to ₹10 lakh fine
66F	Cyberterrorism	Life imprisonment

Figure 5: Punishment and Legal Consequences

10.ASSIGNMENT 1- UNIT 1

SET 1. Discuss the importance of cybersecurity in modern organizations. Explain how the principles of the CIA Triad (Confidentiality, Integrity, Availability) help ensure a secure information environment.

SET 2. Create a chart that categorizes different types of cybercriminals. For each type, mention: Motivation, Common tools used, Typical targets and One real-world example

SET 3: Prepare a timeline showing the evolution of cybercrime from the 1980s to the present. Include at least 5 major events or milestones. For each event, briefly explain its significance in cybersecurity history.

SET4: Compare and contrast the Indian IT Act with at least one other country's cyber law framework (e.g., USA's Computer Fraud and Abuse Act). Highlight differences in definitions, punishments, and effectiveness.

SET5: Choose one international cyber attack (e.g., SolarWinds breach, Ukraine power grid attack). Analyze its origin, technique, impact, and how global law enforcement responded.

R.M.K GROUP OF INSTITUTIONS

11.PART A Q & A (WITH K LEVEL AND CO) UNIT 1

1. What is Cybersecurity?

- Cybersecurity refers to the protection of internet-connected systems, including hardware, software, and data, from cyber threats and attacks.

2. Why do organizations need cybersecurity? K1,CO1

- Organizations need cybersecurity to protect sensitive data, ensure business continuity, maintain trust, and prevent financial and reputational loss due to cyber attacks.

3. What does the CIA triad stand for? K2,CO1

- The CIA triad stands for Confidentiality, Integrity, and Availability, which are the three core principles of information security.

4. Define Confidentiality in cybersecurity. K2,CO1

Confidentiality ensures that data is accessible only to authorized users and is protected from unauthorized access.

5. Define Integrity in cybersecurity.K3,CO1

Integrity refers to maintaining the accuracy and consistency of data during its entire lifecycle, preventing unauthorized alterations.

6. Define Availability in cybersecurity. K3,CO1

Availability ensures that authorized users have reliable and timely access to data and systems when needed.

7. Mention any two common reasons for cybercrime. K4,CO1

Financial gain and political motivation are two common reasons for cybercrime.

R.M.K GROUP OF INSTITUTIONS

8. What is cybercrime?. K4,CO1

Cybercrime is any criminal activity that involves a computer, networked device, or a network.

9. Why is cybersecurity critical for businesses today?.K5,CO1

Cybersecurity is crucial because businesses face growing threats such as data breaches, ransomware, and phishing, which can cause massive losses.

10. What was the Morris Worm, and why is it significant? K5,CO1 (GATE)

The Morris Worm, released in 1988, was one of the first internet worms that caused major system disruptions and led to new cybersecurity laws.

11. What is ransomware, and how does it affect users?K1,CO1

Ransomware encrypts a victim's data and demands a ransom for decryption. It can lock out users and disrupt critical services.

12. Explain the term "phishing" with an example.K1,CO1

Phishing is a cybercrime where attackers trick users into revealing sensitive information, often through fake emails that mimic legitimate sources.

13. Who are known as "script kiddies" in cybercrime? K2,CO1

Script kiddies are unskilled individuals who use pre-made hacking tools and scripts to carry out cyber attacks without technical knowledge.

14. Who is considered a hacktivist? K2,CO1

A hacktivist is someone who hacks systems for political or social reasons, aiming to bring attention to a cause or ideology.

R.M.K GROUP OF INSTITUTIONS

15. What is an insider threat in cybersecurity? K3,CO1

An insider threat is a security risk originating from within an organization, often involving employees misusing access for malicious purposes.

16. How do state-sponsored cybercriminals operate? K3,CO1

State-sponsored cybercriminals are funded by governments to perform espionage, sabotage, or disrupt services in other countries or rival organizations.

17. Define cyber terrorism with an example.. K4,CO1

Cyber terrorism involves using computer-based attacks to cause fear, disruption, or damage to critical infrastructure like power grids or transport systems.

18. What are the objectives of cyber laws in India?K4,CO1

Cyber laws in India aim to regulate digital activities, prevent cybercrimes, protect data privacy, and enable legal action against cyber offenders.

19. What does Section 66 of the IT Act 2000 cover? K5,CO1 (GATE)

Section 66 covers computer-related offenses such as hacking and unauthorized access, and prescribes penalties including imprisonment and fines.

20. What is Section 43 of the IT Act concerned with? K5,CO1

Section 43 deals with unauthorized access and damage to computers, networks, or data, even if done without malicious intent.

21. What does Section 66C of the IT Act specify? (K1,CO1)

Section 66C addresses identity theft, where someone fraudulently uses another person's credentials like passwords or digital signatures for gain.

R.M.K GROUP OF INSTITUTIONS

22. What is the role of CERT-In in India? (K2.CO1) (GATE)

CERT-In is the national agency responsible for responding to cybersecurity threats, issuing advisories, and coordinating cyber incident responses in India.

23. What measures can organizations take to prevent cybercrimes?(K3)

Organizations can prevent cybercrimes through firewalls, encryption, employee training, regular audits, and implementation of strong access control policies.

24. Mention two global cyber attacks. (K4)

- ❖ WannaCry ransomware attack (2017)
- ❖ The SolarWinds supply chain attack (2020).

25. What is cyber espionage? (K2)

Cyber espionage involves unauthorized access to confidential data for political or military advantage, usually by state-sponsored attackers.

R.M.K GROUP OF INSTITUTIONS

12.PART B Q s (WITH K LEVEL AND CO) UNIT 1

1. Explain the need for cybersecurity in modern organizations.(13) **K2,CO1**
2. Describe the CIA Triad and its role in enterprise cybersecurity..(13) **K2,CO1**
3. Analyze the reasons behind cybercrime and its impact on organizations and individuals. (13) **K4,CO1**
4. Trace the evolution of cybercrime with key historical incidents. (15) **K3,CO1**
5. Classify cybercriminals based on their intent, skill level, and methods..(8) **K3,CO1**
6. Write a detailed note on the global perspective of cybercrime..(15) **K2,CO1**
7. Explain the key provisions of the Indian IT Act related to cybercrime..(13) **K2,CO1**
8. Discuss the role of cyber laws and law enforcement in reducing cybercrimes.

13. Supportive online Certification courses

1. Udacity: **ENTERPRISE CYBER SECURITY**

   https://www.udacity.com/course/enterprise-security-nanodegree--nd0035

2. NPTEL: **ENTERPRISE CYBER SECURITY**

   https://onlinecourses.nptel.ac.in/noc23_cs127/preview

R.M.K GROUP OF INSTITUTIONS

14. Real time applications in day to day life and to Industry

❖ Burp Suite

Companies that want to run security tests on web apps should use this service. It includes various hacker applications that operate together to support the entire pen-testing procedure. It has everything from the initial mapping to analyzing an app's attack surface.

➢ Burp Suite has the following features:

✓ A prominent ethical hacking software that discovers over 3000 online application flaws.

✓ Examines custom apps as well as open-source software and code.

✓ It comes with an easy-to-use Login Sequence Recorder that enables automated scanning.

✓ Its built-in vulnerability management examines data safety.

✓ It detects key network vulnerabilities with 100 percent precision.

✓ Easily generates a wide range of compliance and technical data.

✓ Scanning and crawling capabilities are automated.

❖ Metasploit

Metasploit is a hacking framework that focuses on ethical hacking. It's an open-source ethical hacking app. The framework is built with Ruby, and ethical hackers use it to find flaws and write code to fix them.

➢ Metasploit's key features include:

✓ How to get past detecting systems.

✓ Attacks that are launched from afar.

✓ There is a list of all networks and hosts.

✓ Scanning for vulnerabilities using various methods.

R.M.K GROUP OF INSTITUTIONS

15. ASSESSMENT SCHEDULE

Tentative schedule for the Assessment During 2021-2022 ODD semester

S.NO	Name of the Assessment	Start Date	End Date	Portion
1	Unit Test 1			UNIT 1
2	IAT 1			UNIT 1 & 2
3	Unit Test 2			UNIT 3
4	IAT 2			UNIT 3 & 4
5	Revision 1			UNIT 5 , 1 & 2
6	Revision 2			UNIT 3 & 4
7	Model			ALL 5 UNITS

R.M.K GROUP OF INSTITUTIONS

R.M.K GROUP OF INSTITUTIONS

16. PRESCRIBED TEXT BOOKS & REFERENCE BOOKS

TEXT BOOKS:

1. Anand Shinde, "Introduction to Cyber Security Guide to the World of Cyber Security", Notion Press, 2021.
2. Network Security Essentials (Applications and Standards) by William Stallings Pearson Education, 2018.

REFERENCES:

1. William Stallings, "Cryptography and Network Security - Principles and Practice", Seventh Edition, Pearson Education, 2017.
2. Ravi Das and Greg Johnson, "Testing and Securing Web Applications", 2021.
3. Andrew Hoffman, Web Application Security: Exploitation and Countermeasures for Modern Web Applications, O'Reilly Media, Inc, 2020.

R.M.K GROUP OF INSTITUTIONS

17. MINI PROJECT SUGGESTION

SET 1: Analysis of a Real-World Cyber Attack Using the CIA Triad

SET2: Mapping the Evolution of Cybercrime: A Timeline Project

SET3: Comparative Study of Cyber Laws in India and Another Country

SET4: Cybercrime Classification and Mitigation Strategy Design

SET5: Simulation: Phishing Attack and Detection Techniques

R.M.K GROUP OF INSTITUTIONS

18. GATE QUESTIONS

1. Which of the following best describes the components of the CIA Triad in cybersecurity?
A) Control, Integrity, Audit
B) Confidentiality, Integrity, Availability
C) Confidentiality, Identity, Authentication
D) Control, Information, Access
✓ Answer: B) Confidentiality, Integrity, Availability

2. Which of the following can be considered threats to the Availability component of the CIA triad?
A) Denial-of-Service (DoS) attack
B) Data tampering
C) Hardware failure
D) Power outage
✓ Answer: A, C, D

3. Which of the following is NOT a commonly accepted motivation behind cyber crimes?
A) Financial Gain
B) Political Agenda
C) Personal Curiosity
D) Physical Assault
✓ Answer: D) Physical Assault

4. The need for cybersecurity in modern organizations has increased due to:
A) Growing use of paper-based records
B) Decrease in digital transactions
C) Rising incidents of malware, phishing, and data breaches
D) Stable and threat-free digital environments
✓ Answer: C) Rising incidents of malware, phishing, and data breaches

5. Which of the following is considered a type of cyber criminal?
A) White hat hacker
B) Script kiddie
C) Hacktivist
D) All of the above
✓ Answer: D) All of the above

6. Which of the following crimes can be classified under cybercrimes against individuals?
A) Identity Theft
B) Cyberstalking
C) Cyberterrorism
D) Credit Card Fraud
✓ Answer: A, B, D

Thank you

Disclaimer:

This document is confidential and intended solely for the educational purpose of RMK Group of Educational Institutions. If you have received this document through email in error, please notify the system manager. This document contains proprietary information and is intended only to the respective group / learning community as intended. If you are not the addressee you should not disseminate, distribute or copy through e-mail. Please notify the sender immediately by e-mail if you have received this document by mistake and delete this document from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.