NEERAJ®

# SECURITY AND CYBER LAWS

## M.C.S.-215

**Chapter Wise Reference Book Including Solved Sample Papers**

By: *Anand Prakash Srivastava*

*Based on*

## I.G.N.O.U.

**& Various Central, State & Other Open Universities**

Serving Education for Last 40 Years

**NEERAJ PUBLICATIONS**
*(Publishers of Educational Books)*

**Retail Sales Office:**
**1507, 1st Floor, Nai Sarak, Delhi - 6**
**Mob.: 8510009872, 8510009878**
**E-mail: info@neerajbooks.com**
**Website: www.neerajbooks.com**

MRP ₹ 240/-

Published by:

**NEERAJ**
**PUBLICATIONS**

*(Publishers of Educational Books)*

Retail Sales Office : 1507, 1st Floor, Nai Sarak, Delhi-110 006
E-mail: info@neerajbooks.com | Website: www.neerajbooks.com

Typesetting by: Competent Computers, Printed at: Novelty Printing Press

*Disclaimer/T&C*

1. *For the best & up-to-date study & results, please prefer the recommended textbooks/study material only.*
2. *This book is just a Guide Book/Reference Book published by NEERAJ PUBLICATIONS based on the suggested syllabus by a particular Board/University.*
3. *These books are prepared by the author for the help, guidance and reference of the student to get an idea of how he/she can study easily in a short time duration. Content matter & Sample answers given in this Book may be Seen as the Guide/Reference Material only. Neither the publisher nor the author or seller will be responsible for any damage or loss due to any mistake, error or discrepancy as we do not claim the Accuracy of these Solutions/Answers. Any Omission or Error is highly regretted though every care has been taken while preparing, printing, composing and proofreading of these Books. As all the Composing, Printing, Publishing and Proof Reading, etc., are done by Human only and chances of Human Error could not be denied. Any mistake, error or discrepancy noted may be brought to the publishers notice which shall be taken care of in the next edition and thereafter as a good gesture by our company he/she would be provided the rectified Book free of cost. Please consult your Teacher/Tutor or refer to the prescribed & recommended study material of the university/board/institute/ Govt. of India Publication or notification if you have any doubts or confusions regarding any information, data, concept, results, etc. before you appear in the exam or Prepare your Assignments before submitting to the University/Board/Institute.*
4. *In case of any dispute whatsoever the maximum anybody can claim against NEERAJ PUBLICATIONS is just for the price of the Book.*
5. *The number of questions in NEERAJ study materials are indicative of general scope and design of the question paper.*
6. *Any type of ONLINE Sale/Resale of "NEERAJ BOOKS" published by "NEERAJ PUBLICATIONS" on Websites, Web Portals, Online Shopping Sites, like Amazon, Flipkart, Ebay, Snapdeal, etc., is strictly not permitted without prior written permission from NEERAJ PUBLICATIONS. Any such online sale activity by an Individual, Company, Dealer, Bookseller, Book Trader or Distributor will be termed as ILLEGAL SALE of NEERAJ BOOKS and will invite legal action against the offenders.*
7. *The User agrees Not to reproduce, duplicate, copy, sell, resell or exploit for any commercial purposes, any portion of these Books without the written permission of the publisher. This book or part thereof cannot be translated or reproduced in any form (except for review or criticism) without the written permission of the publishers.*
8. *All material prewritten or custom written is intended for the sole purpose of research and exemplary purposes only. We encourage you to use our material as a research and study aid only. Plagiarism is a crime, and we condone such behaviour. Please use our material responsibly.*
9. *All matters, terms & disputes are subject to Delhi Jurisdiction only.*

# CONTENTS

# SECURITY AND CYBER LAWS

| *S.No.* | *Chapter* | *Page* |
|---|---|---|

## BLOCK-1 : CYBER SECURITY ISSUES

## BLOCK-2 : CYBER LAWS

■■

# Sample Preview of the Solved Sample Question Papers

*Published by:*

NEERAJ
PUBLICATIONS
www.neerajbooks.com

# *Sample* QUESTION PAPER-1

*( Solved )*

## SECURITY AND CYBER LAWS

**M.C.S.- 215**

*Time: 3 Hours ]* *[ Maximum Marks: 100*

***Note:*** *Attempt any **five** questions. All questions carry equal marks.*

**Q. 1. What is Phishing and whether it is challenge to digital security?**

**Ans. Ref.:** See Chapter-1, Page No. 7, Q. No. 2.

**Q. 2. A RSA cryptosystem uses two prime numbers 3 and 13 to generate the public key = 3 and the private key = 7. What is the value of cipher text for a plain text?**

**Ans. Ref.:** See Chapter-2, Page No. 39, Q. No. 8.

**Q. 3. What is availability and integrity?**

**Ans. Ref.:** See Chapter-3, Page No. 64, Q. No. 1.

**Q. 4. Describe the need for regulation of cyberspace?**

**Ans. Ref.:** See Chapter-4, Page No. 89, Q. No. 1.

**Q. 5. Discuss is brief the Penalty and Compensation.**

**Ans. Ref.:** See Chapter-5, Page No. 115, Q. No. 1.

**Q. 6. What is meant by domain name?**

**Ans. Ref.:** See Chapter-6, Page No. 139, Q. No. 2.

**Q. 7. Explain the reasons for commission of cyber crimes.**

**Ans. Ref.:** See Chapter-1, Page No. 9, Q. No. 2.

**Q. 8. Write short notes on the following:**

***(a)*** **Digital Certificates**

**Ans. Ref.:** See Chapter-2, Page No. 31, 'Digital Certificates'.

***(b)*** **Computer**

**Ans. Ref.:** See Chapter-3, Page No. 61, 'Computer'.

***(c)*** **UNESCO**

**Ans. Ref.:** See Chapter-4, Page No. 89, 'UNESCO'.

***(d)*** **Offences**

**Ans. Ref.:** See Chapter-5, Page No. 110, 'Offences'.

■■

# *Sample* QUESTION PAPER-2

*( Solved )*

## SECURITY AND CYBER LAWS

**M.C.S.- 215**

*Time: 3 Hours ]* *[ Maximum Marks: 100*

***Note:*** *Attempt any **five** questions. All questions carry equal marks.*

**Q. 1. A RSA cryptosystem uses two prime numbers, 3 and 11, to generate private key = 7. What is the value of cipher text for a plain text 5 using the RSA public-key encryption algorithm?**

**Ans. Ref.:** See Chapter-2, Page No. 40, Q. No. 9.

**Q. 2. Discuss how cyberspace can be regulated.**

**Ans. Ref.:** See Chapter-4, Page No. 90, Q. No. 2.

**Q. 3. Discuss in brief the sections comes under Appellate Tribunal.**

**Ans. Ref.:** See Chapter-5, Page No. 115, Q. No. 2.

**Q. 4. Name any three cyber security software to fight against cyber-attacks?**

**Ans. Ref.:** See Chapter-1, Page No. 8, Q. No. 3.

**Q. 5. Enlist copyright issues in cyberspace.**

**Ans. Ref.:** See Chapter-6, Page No. 139, Q. No. 3.

**Q. 6. How many types of cyber crime? Explain it.**

**Ans. Ref.:** See Chapter-1, Page No. 9, Q. No. 3.

**Q. 7. What are the various types of cyber threats?**

**Ans. Ref.:** See Chapter-3, Page No. 64, Q. No. 2.

**Q. 8. Write short notes on the following:**

***(a)*** **Hash Functions**

**Ans. Ref.:** See Chapter-2, Page No. 32, 'Hash Functions'.

***(b)*** **Mobile**

**Ans. Ref.:** See Chapter-3, Page No. 61, 'Mobile'.

***(c)*** **Cyberbrics**

**Ans. Ref.:** See Chapter-4, Page No. 89, 'Cyberbrics'.

***(d)*** **Reverse Steganography**

**Ans. Ref.:** See Chapter-5, Page No. 113, 'Reverse Steganography'.

■■

# SECURITY AND CYBER LAWS

## BLOCK-1 : CYBER SECURITY ISSUES

## Cyber Security Issues and Challenges

1

### INTRODUCTION

Information Technology (IT) is the application of computers and tele-communications equipment to store, retrieve, transmit and manipulate data, often in the context of a business or other enterprise.

Cyber security can be a useful term but tends to defy precise definition. It is also sometimes inappropriately conflated with other concepts such as privacy, information sharing, intelligence gathering, and surveillance. However, cyber security can be an important tool in protecting privacy and preventing unauthorized surveillance, and information sharing and intelligence gathering can be useful tools for effecting cyber security.

The term is commonly used as a synonym for computers and computer networks, but it also encompasses other information distribution technologies such as television and telephones. Several industries are associated with information technology, including computer hardware, software, electronics, semiconductors, internet, tele-communications equipment, engineering, healthcare, e-commerce and computer services.

The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an Act of the Indian Parliament (No. 21 of 2000) notified on 17 October, 2000. It is the primary law in India dealing with cybercrime and electronic commerce.

### CHAPTER AT A GLANCE

### DIGITAL SECURITY: PROS AND CONS

Digital Security is important because it allows people to use social media and online banking and protects them from risks such as identity theft and fraud. If the steps mentioned earlier are followed, then your digital security is strong and will protect your information.

The three components of the CIA triad are discussed below:

**Confidentiality:** This component is often associated with secrecy and the use of encryption. Confidentiality in this context means that the data is only available to authorized parties.

**Integrity:** Data integrity refers to the certainty that the data is not tampered with or degraded during or after submission.

**Availability:** This means that the information is available to authorized users when it is needed.

**Digital Security: Pros**

1. Protects system against viruses, worms, spyware and other unwanted programs.
2. Protection against data from theft.
3. Protects the computer from being hacked.
4. Minimizes computer freezing and crashes.
5. Gives privacy to users.

**Digital Security Cons**

1. Firewalls can be difficult to configure correctly.
2. Incorrectly configured firewalls may block users from performing certain actions on the Internet, until the firewall configured correctly.
3. Makes the system slower than before.
4. Need to keep updating the new software in order to keep security up to date.
5. Could be costly for average user.

### SECURITY ISSUES /BREACHES IN CYBERSPACE

Cyber security professionals continually defend computer systems against different types of cyber threats. Cyber attacks hit businesses and private systems every day, and the variety of attacks has increased quickly. According to former Cisco CEO John

Chambers, "There are two types of companies: those that have been hacked, and those who don't yet know they have been hacked."

Following are the most common security issues witnessed in cyberspace in recent past:

**1. Unauthorized Access:** Unauthorized Access is when a person who does not have permission to connect to or use a system gains entry in a manner unintended by the system owner. The popular term for this is "hacking".

Here is one example scenario. Someone walks into a car dealership intending to purchase a car and finance it using your name and personal information. The dealer obtains a copy of your credit report to ensure you can make the payments. The credit report the dealer receives will have the fraud alert flag on it. The dealer then knows he should contact you to confirm you are indeed the person wanting to purchase the car. When you inform the dealer that you are not purchasing a car from him, the line of credit isn't issued.

This alert only influences new lines of credit. Existing lines of credit are not affected, so you can continue to use your credit cards, pay on loans, etc, without any problems.

**2. Distributed Denial of Service Attack**: A Denial of Service (DoS) is a type of cyber attack that floods a computer or network so it can't respond to requests. A distributed DoS (DDoS) does the same thing, but the attack originates from a computer network. Cyber attackers often use a flood attack to disrupt the "handshake" process and carry out a DoS.

Some common examples of DDoS attacks are UDP flooding, SYN flooding and DNS amplification.

**3. Malwares:** Malware is malicious software such as spyware, ransom ware, viruses and worms. Malware is activated when a user clicks on a malicious link or attachment, which leads to installing dangerous software. Cisco reports that malware, once activated, can:

- Block access to key network components (ransom ware)
- Install additional harmful software
- Covertly obtain information by transmitting data from the hard drive (spyware)
- Disrupt individual parts, making the system inoperable

**Covid Lock ransomware is an example:** This type of ransomware infects victims via malicious files promising to offer more information about the disease. The problem is that, once installed, Covid Lock encrypts data from Android devices and denies data access to victims

**4. Social Engineering Attacks:** Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information. Social engineering attacks happen in one or more steps.

**Example of Social Engineering Attacks**

**Shark Tank, 2020**

Shark Tank television judge Barbara Corcoran was tricked in a nearly USD 400,000 phishing and social engineering scam in 2020. A cybercriminal impersonated her assistant and sent an email to the bookkeeper requesting a renewal payment related to real estate investments. He used an e-mail address similar to the legitimate one. The fraud was only discovered after the bookkeeper sent an e-mail to the assistant's correct address asking about the transaction.

**5. Phishing:** Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through e-mail.

**Example of E-mail Phishing**

The Daily Swig reported a phishing attack that occurred in December 2020 at US healthcare provider Elara Caring that came after an unauthorized computer intrusion targeting two employees. The attacker gained access to the employees' e-mail accounts, resulting in the exposure of the personal details of over 100,000 elderly patients, including names, birth dates, financial and bank information, Social Security numbers, driver's license numbers and insurance information. The attacker maintained unauthorized access for an entire week before Elara Caring could fully contain the data breach.

**6. Crypto Jacking:** Crypto jacking is malicious crypto mining that happens when cybercriminals hack into business and personal computers, laptops, and mobile devices to install software. This software uses the computer's power and resources to mine for crypto currencies or steal crypto currency wallets owned by unsuspecting victims.

**Examples of Crypto Jacking**

In February 2018, a Spanish cyber security firm, Panda Security, announced that a crypto jacking script, known by its nickname "WannaMine," had spread to computers around the world. The new malware variant was being used to mine the cryptocurrency Montero.

**7. Exploiting Vulnerability:** An exploit is any attack that takes advantage of vulnerabilities in applications, networks, operating systems, or hardware.

**Example of Exploiting Vulnerability:** "Europe's biggest phone company identified hidden backdoors in the software that could have given Huawei unauthorized access to the carrier's fixed-line network in Italy, a system that provides internet service to millions of homes and businesses… Vodafone asked Huawei to remove backdoors in home internet routers in 2011 and received assurances from the supplier that the issues were fixed, but further testing revealed that the security vulnerabilities remained."

**8. Cyber Physical Attacks:** A security breach in cyber space those impacts on the physical environment.

**Example of Cyber Physical Attacks**

In July 2016, a Japanese travel agency, JTB Corp, suffered a data breach compromising almost 93 million user records. The data breach was a result of an employee opening a malicious document which he received via a phishing e-mail. The malicious document included a Trojan horse that is designed to steal user information. It was reported that 7.93 million user records from Japanese Travel Agency were compromised.

**9. Internet of Things (IOT) Attacks:** IoT attacks happen when bad actors try to compromise the security of an Internet of Things (IoT) device or network. When devices are compromised, attackers can steal or manipulate sensitive data, join IoT devices to a botnet, or take control of a system.

**Example of Internet of Things (IOT) Attacks**

Back in October of 2016, the largest DDoS attack ever was launched on service provider Dyn using an IoT botnet. This lead to huge portions of the internet going down, including Twitter, the Guardian, Netflix, Reddit, and CNN.

This IoT botnet was made possible by malware called Mirai. Once infected with Mirai, computers continually search the internet for vulnerable IoT devices and then use known default usernames and passwords to log in, infecting them with malware. These devices were things like digital cameras and DVR players.

**10. Web Jacking:** Illegally seeking control of a website by taking over a domain is known as Web Jacking. In web jacking attack method hackers compromises with the Domain Name System (DNS) that resolves website URL to IP address but the actual website is never touched.

**Example of Web Jacking**

Recently the site of MIT (Ministry of Information Technology) was hacked by the Pakistani hackers and some obscene matter was placed therein. Further the site of Bombay crime branch was also web jacked. Another case of web jacking is that of the 'gold fish' case.

**11. Drive by download:** Drive by download attacks specifically refer to malicious programs that install to your devices – without your consent. This also includes unintentional downloads of any files or bundled software onto a computer device.

Some of the common security issues witnessed in cyberspace in recent past are as follows:

**1. Internet time theft:** It refers to the theft in a manner where the unauthorized person uses internet hours paid by another person.

**2. Key Loggers:** Key loggers are activity-monitoring software programs that give hackers access to your personal data.

**3. Website defacement:** Web defacement is an attack in which malicious parties penetrate a website and replace content on the site with their own messages

**4. Pharming:** Pharming, a portmanteau of the words "phishing" and "farming", is an online scam similar to phishing, where a website's traffic is manipulated, and confidential information is stolen.

**5. Phreaking:** Hackers attacking your voice network like they would (and do) attack your data network.

**6. E-mail bombing:** An e-mail bomb is a form of Internet abuse which is perpetrated through the sending of massive volumes of e-mail to a specific e-mail address with the goal of overflowing the mailbox and overwhelming the mail server hosting the address, making it into some form of denial of service attack.

## TECHNOLOGY'S ANSWERS TO CYBER SECURITY

**1. Unauthorized Access:** Unauthorized access is when someone gains access to a website, program, server, service, or other system using someone else's account or other methods. For example, if someone kept guessing a password or username for an account that was not theirs until they gained access, it is considered unauthorized access.

**2. Distributed Denial of Service Attack:** DDoS (Distributed Denial of Service) is a category of malicious cyber-attacks that hackers or cybercriminals employ in order to make an online service, network resource or host machine unavailable to its intended users on the Internet.

**3. Malwares:** Malware is a program designed to gain access to computer systems, normally for the benefit of some third party, without the user's permission. Malware includes computer viruses, worms, Trojan horses, ransom ware, spyware and other malicious programs.

***(a)* Botnets:** A botnet (short for "robot network") is a network of computers infected by malware that are under the control of a single attacking party, known as the "bot-herder." Each individual machine under the control of the bot-herder is known as a bot. They are also used to spread bots to recruit more computers to the botnet.

***(b)* Ransom wares:** Ransom ware grasps a computer system or the data it contains until the victim makes a payment. Ransom ware encrypts data in the computer with a key which is unknown to the user. The user has to pay a ransom (price) to the criminals to retrieve data. Once the amount is paid the victim can resume using his/her system.

***(c)* Trojan:** A Trojan horse is malware that carries out malicious operations under the appearance of a desired operation such as playing an online game. A Trojan horse varies from a virus because the Trojan binds itself to non-executable files, such as image files and audio files.

***(d)* Virus:** A virus is a malicious executable code attached to another executable file. The virus spreads when an infected file is passed from system to system. Viruses can be harmless or they can modify or delete data. Opening a file can trigger a virus. Once a program virus is active, it will infect other programs on the computer.

***(e)* Worms:** Worms replicate themselves on the system, attaching themselves to different files and looking for pathways between computers, such as computer network that shares common file storage areas. Worms usually slow down networks. A virus needs a host program to run but worms can run by themselves. After a worm affects a host, it is able to spread very quickly over the network.

**4. Spywares:** Its purpose is to steal private information from a computer system for a third party. Spyware collects information and sends it to the hacker.

**5. Social Engineering Attacks:** Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. In cybercrime, these "human hacking" scams tend to lure unsuspecting users into exposing data, spreading malware infections, or giving access to restricted systems.

**6. Phishing:** Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through e-mail. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine.

**7. Cryptojacking:** we are announcing the integration of Intel Threat Detection Technology (TDT) into Microsoft Defender for Endpoint, an addition that enhances the detection capability and protection against crypto jacking malware.

**8. Exploiting Vulnerability:** Vulnerabilities can be exploited by a variety of methods including SQL injection, buffer overflows, cross-site scripting (XSS) and open-source exploit kits that look for known vulnerabilities and security weaknesses in web applications.

**9. Cyber Physical Attacks:** Assess your vulnerability risk to a cyber attack, Identify and protect sensitive business and personal information, Establish a secure backup system, Monitor for and have a plan to react to security incidents, Provide security training, etc.

**10. IOT Attacks:** Change default router settings. Most people forget to rename the router and stick to the name given by the manufacturer, Disconnect IoT devices when they are not needed and Pick a strong password and do not overuse it.

**11. Web Jacking:** Users who receive emails with phishing links should always check the URL first by typing the URL in the address bar rather than clicking the link. If the URL does not match the expected website, the user should not click on the link and should also not click on any suspicious links in e-mails. Users should also avoid clicking on links sent in e-mails with an embedded image or if the sender starts with a link that looks like a typical URL.

**12. Drive by Download:** Update your software quickly and constantly, Remove unnecessary software and plug-ins, Stop using a privileged account for day-to-day work, Use a firewall and Use web-filtering software etc. can provide the protection against the drive by download.

**Cyber Security Intrusion Detection**

An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and