Introduction to Computer Security

Introduction

Computer becomes part of our daily life. We use computer to perform many of our daily repetitive tasks. We store a significant amount of our personal data like photographs, copy of Aadhaar card, bank details, school projects, assignments, etc. on devices like desktop computers, laptops and smart phones. These data can be misused by someone like hackers for their personal benefits. Hence it is important for us to protect such data from unauthorized use. By learning the computer security fundamentals, we can better protect our computer systems and data from harm, theft, and misuse. This chapter helps to learn the essential concepts of computer security. Throughout this chapter, students will learn importance of the computer security, major cyber threats, key security mechanisms, and general computer security guidelines specifically designed for students.

Need of Computer Security

Today, we heavily depend on computer usage to store our personal data. When we use a computer, we focus only on the software relevant to our tasks. However, there are many other components and processes working in the background that play a crucial role, especially from a security point of view. A computer system also involves various actors such as regular users, hackers, and hidden programs like viruses and worms. Security features like antivirus software and system settings are constantly working to protect the system. It is important to understand all these additional elements as shown in figure 11.1 to ensure the overall security of your computer.

Figure 11.1 Additional Elements of Today's Computer System

It is very important for us to understand basic computer security techniques to protect our digital resources from misuse by hackers. Let us understand why computer security is important and what we can do to protect our digital resources from cyber attacks.

Why Computer Security is Important?

Computer security is essential because we depend on technology for everyday activities like schoolwork, social media communication, online banking, shopping, and entertainment. By learning about computer security, we can protect our personal and sensitive information, and create a safer digital environment.

Origins of Computer Security

The concept of computer security was not a concern during the early days of computer usage. Computers were initially large, isolated machines used by a limited group of individuals. However, as technology evolved and interconnected computer systems emerged, the need for security became

apparent. The development of the internet in the late 20th century was a turning point, as it opened up new opportunities along with challenges.

The Evolution of Cybersecurity

Nowadays, computer security is commonly referred to as cybersecurity. This field focuses on protecting computers, smartphones, networks, and data from unauthorized access by attackers, known as hackers. The evolution of cybersecurity began along with the rise of computer networks. As the internet grew in the 1990s, cyber threats like viruses, worms, and hacking became more common. Usage of the internet brought new types of challenges. The computer based malicious programs like viruses started creating problems for many internet users. This led to the birth of cybersecurity, a field dedicated to developing strategies and technologies to defend against various types of cyber problems.

Important Digital Resources

In the context of computer security, "digital resources" refers to anything that exists in a digital format and holds some value, which needs protection from unauthorized access or attacks. Table 11.1 outlines some of the key digital resources that individuals, schools, governments, and businesses need to safeguard against potential attackers.

Category	Digital Resources That Need Protection
Individuals	Phone numbers, residence address, email addresses, bank account numbers, debit/credit card details, UPI IDs, identity cards (Aadhaar, PAN, Passport, Driving License), personal photographs and videos, biometric details (fingerprints, face ID), social media account IDs, etc.
Schools	Student and teacher contact details, attendance records, academic results, digital question papers and answer sheets, e-learning platforms, apps and their usernames/passwords, school websites, fee payment data, school networks and Wi-Fi passwords, etc.
Government	Aadhaar and other ID databases, election records, income tax records, health data, passport/immigration data, ration cards, pensions, land and property records, digital maps, secret information related to defence, etc.
Businesses	Bank details, customer data (names, emails, phone numbers), employee records and salary details, business emails, websites and apps, loans/ investments details, business secrets, vendor details, etc.

Table 11.1 : Important Digital Resources

All of these digital resources require protection not only from hackers but also from accidental damage, insider attacks by employees, business competitors, and international attacks.

Data Privacy and Protection

It is crucial for us to understand data privacy and protection, especially since we rely heavily on smart phone in daily lives.

Data privacy refers to the practice of securing personal information such as names, addresses, and school records, against unauthorized access and misuse. Protecting this data is vital for maintaining our privacy and ensuring that our information does not fall into the wrong hands.

Why Data Privacy Matters for Students

Understanding data privacy is crucial for students as mostly they are not aware about the dark side of the fancy internet world. Maintaining data privacy helps in protecting identity and personal information from cyber criminals who may attempt to exploit it for malicious purposes. Being aware of data privacy means:

- Being cautious about what you share online.
- Understanding the privacy settings on our social media accounts.
- Recognizing the importance of strong and unique passwords.

Role of Schools and Students in Data Protection

Schools play a crucial role in data protection by implementing secure systems for managing student information, conducting regular security audits, and educating students on responsible online behavior.

As students, you can contribute to data protection by:

- Being mindful of the information you share.
- Using secure Wi-Fi networks.
- Reporting any suspicious activities to a trusted adult or your teacher.

Students can help to create a safer digital environment for themselves and their family members by educating themselves about data privacy and protection techniques.

Introduction to Cyber Security

Cybersecurity involves safeguarding computers, smartphones, networks, and data from unauthorized access. It ensures that the digital information we use and share is protected from threats such as hackers and viruses. For students, cybersecurity means learning how to keep personal information secure, being aware of potential online dangers, and understanding the importance of strong passwords and safe online practices. By grasping the basics of cybersecurity, students can surf the digital world safely, engage in secure online activities, and develop skills to protect themselves and their communities.

Basic Do's and Don'ts of Cybersecurity

Understanding and implementing effective cybersecurity habits is essential for us to protect our safety and privacy in the digital world. By following the basic do's and don'ts given in table 11.2, we can greatly minimize chances of becoming victims of cyber-attacks.

Aspects	Do's	Don'ts
Personal Information	Keep your data private on social media platforms. If required, share minimal data.	Avoid posting full name, address, phone number and birth date on social media and public websites.
User IDs	Use a different user IDs (username) for each online accounts wherever possible.	Avoid using your email address as a username, as it helps attackers to find your other online accounts.
Passwords	Use strong, unique passwords for each account. To create a strong password, use combination of uppercase and lowercase letters, numbers, and symbols. For example, "P@ndas$5Rocks" is a strong password.	Never use easy-to-guess passwords like your name, birthday, or "abc123". Don't use same password for multiple accounts. Avoid writing passwords on paper. "panda123" is an example of a weak password.
Two-Factor Authentication (2FA)	Enable 2FA on all your accounts, especially email, banking and social media accounts.	Never share your 2FA codes like One-Time-Password (OTP) with anyone.
Public Wi-Fi	Only access HTTPS sites while using public Wi-Fi. Also, ensure your home Wi-Fi is password-protected.	Avoid using banking or shopping accounts on public Wi-Fi. Avoid connecting unknown Wi-Fi networks. Hackers may steal our data.
Software Updates	Install software updates for operating system, web browser, and Apps as soon as they are available.	Don't ignore software updates alerts.
Links and Emails	Verify sender details before opening links or attachments. Hover over a link to see the actual URL before clicking it.	Avoid clicking links from unknown SMS and email senders, and don't share personal data in response to unfamiliar requests.
App Downloads	Download apps only from official app stores like Google Play Store and Apple App Store.	Never download apps or .APK files from third-party sources. Don't grant unnecessary permissions to any apps (e.g., a flashlight app requesting access to your contacts).
Security Alerts	Pay attention to security alerts from operating system and antivirus software, and act on them promptly.	Never dismiss or ignore any security alerts without understanding the potential risks.
Backup	Take regular backups of important data files. Store backups in different places (e.g., cloud, external disks and pen drives).	Disconnect backup drives from computers after taking backups. Don't keep it connected.
Cyberbullying	If encountering cyberbullying, report it to a teacher and parent.	Don't engage with cyberbullies by resonding or reacting.
Suspicious Activity	Report any suspicious activity on your accounts or devices immediately to teacher and your parents.	Don't ignore any unusual login attempts or very small financial transactions in online accounts.

Table 11.2: Basic Do's and Don'ts of Cybersecurity

Safe Browsing Habits for Students

Navigating the internet websites safely is crucial for all of us to protect our personal information and maintain privacy online. Being aware of safe browsing habits helps us to avoid cyber threats, such as malware and phishing.Followings are some key practices for safe browsing:

- **Use the Latest Web Browser:** Always keep your web browser updated to the latest version to benefit from the latest security features and patches.
- **Look for HTTPS:** When visiting websites, ensure they use "**HTTPS**" in the URL, indicating a secure connection and our data is encrypted.
- **Avoid Clicking on Unknown Links:** Be cautious of links shared in emails or messages from unknown sources. Hover over links to preview the URL before clicking.
- **Use a Pop-up Blocker:** Enable a pop-up blocker in browser settings to prevent potentially harmful pop-up ads from appearing.
- **Be Skeptical of Free Offers:** Be wary of websites offering free downloads or gifts, as they often contain malware or lead to phishing sites.
- **Logout of Accounts:** Always logout of online accounts when using shared or public computers to prevent unauthorized access.
- **Regularly Clear Cookies and Cache:** Clear your browser's cookies and cache regularly to protect your privacy and improve browser performance.

Students can minimize the risks of cyberattacks by adopting these safe browsing habits, and can enjoy the internet safely.

Introduction to Cyber Threats

A cyber threat is defined as any harmful action aimed at damaging, stealing, or disrupting data, digital systems and networks. In essence, it represents the possibility of a successful cyberattack. Hence, we all need to know about the threats that can harm our computers and personal information. Let us understand the characteristics and some common cyber threats.

Key Characteristics of Cyber Threats

- **Cyber Threat Actors:** They are popularly known as hackers who has some malicious intent. They aim to misuses weaknesses of the system to gain unauthorized access and then misuses victims' data, devices, systems, and networks.
- **Malicious Intent:** They are typically carried out by individuals or groups (hackers) with harmful intentions like financial or non-financial gains.
- **Targeting Vulnerabilities:** Threat actors exploit weaknesses or vulnerabilities in information systems, software, hardware, or even human behavior.
- **Impact on Confidentiality, Integrity, and Availability (CIA Triad):** Cyber threats aim to compromise one or more of these core security principles:
    - Confidentiality: Unauthorized access to sensitive information.
    - Integrity: Unauthorized modification or destruction of data.
    - Availability: Disruption of access to systems or data (e.g., Denial of Service attacks).

  You will learn more about CIA triad in your higher standards.

Types of Cyber Threats

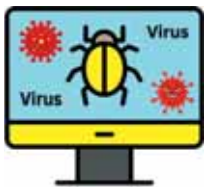
Let us understand common types of the cyber threats.

Malware

It is a type of software designed to damage or gain unauthorized access to a computer system. Malware is a general term used to refer all types of malicious software, such as viruses, worms, Trojans, etc. Malware can be hidden in email attachments or downloads from unreliable websites.

Malware can be classified into various types such as viruses, worms, trojans, ransomware, spyware, adware, and key loggers. These are commonly used by hackers to carry out cyberattacks.

Virus



Viruses are harmful programs that can spread from one computer to another. They attach themselves to files and programs, causing them to run slowly or not at all. Viruses can also corrupt or delete important data files and personal information from your computers.

Worms

Worm is a type of self-replicating malware that spreads across computers and networks without any user action. Unlike viruses, worms do not need to attach themselves to a host program or file.

Trojans

Trojan is a type of malicious software that looks as a legitimate software or file. Trojans often present themselves as helpful software, such as games, utilities, or email attachments. Once activated, it can execute various harmful actions without the user's knowledge.

Ransomware

Ransomware is a type of harmful software that locks - encrypts our data, making it unusable. It can also lock our computer. The attacker then demands money (ransom) to unlock it. It often spreads through fake emails or unsafe downloads. Paying the ransom does not always guarantee that our data or computer will be recovered from attacks.

Spyware

Spyware is a type of malware designed to secretly monitor and collect information about a user's activities on their computer or mobile device.

Adware

Adware is a type of software that automatically displays unwanted advertisements to a user's device, often without user consent. They are not always malicious, but it can slow down your system, consumes internet bandwidth and compromise your privacy.

Keyloggers

Keyloggers are programs designed to capture every keystroke made on our keyboard. These malicious tools can record our usernames, passwords, messages, and various other personal information without our knowledge. Once they have gathered these sensitive details, such programs transmit the information to hackers.

Social Engineering

It is a method used by attackers to trick people into revealing sensitive information, such as passwords, bank details, or personal data, through misleading communications using fake emails, SMSs, phone calls, or even face-to-face conversations. Instead of hacking a computer, the attacker "hacks" the human mind by pretending to be someone you trust, like your teacher, friend, or bank officer. The goal is to gain access to systems or data by exploiting human trust rather than technical weaknesses. For example, a stranger might contact you, pretending to be your teacher, friend, or relatives, asking for your login details, OTP, or bank details while helping you. This is a social engineering trick, which later on can be misused.

Phishing

Phishing is a type of social engineering cyberattack where attackers try to trick people into sharing personal or sensitive information like passwords, credit card numbers, or OTPs by pretending to be a trusted source. It usually happens through fake emails, messages, or websites that look real. These messages often create a sense of urgency, such as saying your account will be blocked unless you act quickly. Following is a phishing example:

- You receive an email that looks like it's from your bank, asking you to click a link and verify your account details. If you click and enter your information the attacker steals it.

Phishing is dangerous because it can lead to identity theft, financial loss, or unauthorized access to accounts. Always double-check links and sender details before responding.

Denial of Service (DoS)

In this category of threat, attackers overwhelms a system with excessive traffic to make it unavailable to genuine users of the systems.

Data Breaches

Data breaches occurs when unauthorized individuals gain access to or expose private data, which can potentially leads to the significant privacy violations and financial losses.

Man-in-the-Middle (MitM)

This type of attacks involve intercepting communications between two parties to steal data without the knowledge of legal parties involved in the communications.

Insider Threats

It involves the malicious acts carried out by individuals who have genuine access to the organization systems, e.g.unhappy-employees.

Zero-day Exploits

Zero-day Exploit is a type of attack that leverage newly discovered websites, apps or games vulnerabilities before a patch or fix is available.

Fake Websites

It's crucial for students to be aware of fake websites, suspicious links, and fake SMSs, as these are common tricks used by cyber criminals to cheat and harm users. Fake websites are designed to look like legitimate sites but are actually fraudulent. These websites aim to steal personal data or install malware on your device.

Example: Imagine you receive an email claiming to be from your favorite online store, offering a massive discount. The email directs you to a website that looks identical to the real online store but is actually a fake website designed to capture your Login-ID and Password.

Security Tip: Always read the website address (URL) carefully. Genuine websites have URLs that start with "https://" and a small padlock icon, indicating a secure connection. In case you have any doubt in the received link, it's safer for you to type the website's address directly into your browser instead of clicking on the received links.

Suspicious Links

Suspicious links are often found in emails, messages, or on websites. Clicking on such links can lead to malware downloads into your system.

Example: You might get a message from a friend on social media with a link saying, “Check out this cool video!” However, the link could lead to a dangerous site that infects your device with malware.

Security Tip: Hover over links to read the actual website address, see where they lead you before clicking. If the URL looks unfamiliar or suspicious, do not click it. Always confirm with the sender if they honestly sent the message.

Fake SMS

Fake SMS, also known as Smishing, are fraudulent text messages that try to trick users into revealing personal information or clicking on malicious links.

Example: You might receive a text message saying you have won a prize and need to click a link to claim it. These messages are often scams meant to steal your information or install harmful software on your phone.

Security Tip: Read carefully when receiving unexpected messages from unknown numbers, particularly those requesting personal information or pressuring you to take immediate action. Never click on links in such messages, and delete them immediately. If required, take advice from your teacher or parents before taking any actions.

Computer Security Mechanisms

Understanding computer security mechanisms is vital for internet users. Computer security mechanisms are tools and techniques designed to protect our devices and personal information from cyber attacks. By learning these security mechanisms, we can safeguard our online activities, ensure digital privacy and safety. Let us understand some of the computer security mechanisms.

Antivirus

Antivirus is a computer program designed to detect and eliminate viruses and other malicious programs from our computer, mobile phone and tablets. It scans files and system regularly to identify threats and remove them before they can cause harm. Keeping antivirus software updated is crucial for maintaining the security of digital devices.

Firewall

A firewall acts as a barrier between our computer and the internet, controlling the incoming and outgoing network traffic. Firewall protects our internal digital resources from outsiders like hackers. It allows only validated and genuine network traffic to enter into our internal computer network. It helps prevent unauthorized access to our system by blocking harmful data and allowing safe data to pass through. Firewalls can be hardware-based, software-based, or a combination of both. See figure 11.2.

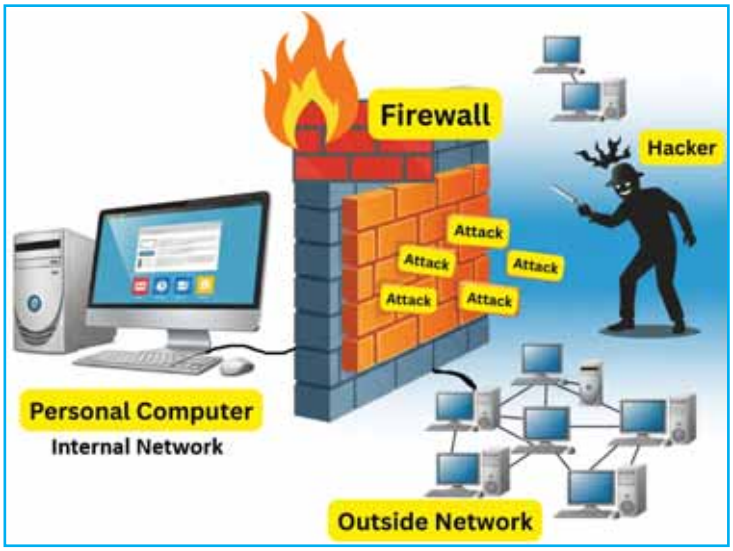


Figure 11.2 : Firewall

Secure Use of Internet and Wi-Fi

Using secure internet connections is important for protecting our data. Avoid using public Wi-Fi for sensitive activities, as these networks are often less secure and more susceptible to cyber-attacks. If you must use public Wi-Fi, consider using a Virtual Private Network (VPN) to encrypt your internet traffic and protect your privacy.

Regular Software Updates

Keeping computer operating system and applications up-to-date is essential for protecting against weaknesses and attacks. Software updates often include security patches that address known threats and weaknesses, ensuring that our device remains protected against the latest cyber threats.

User Education and Awareness

Being aware of potential cyber threats and learning how to recognize and respond to them is a key aspect of computer security. This includes being cautious of phishing scams, fake websites, and suspicious links. Educating yourself and others about safe online practices helps create a more secure digital environment. Students can significantly reduce their risk of falling victim to cyber threats by carefully understanding and implementing computer security mechanisms.

Cyber Crime Portal of Govt. of India

The Government of India has launched a special website called the National Cyber Crime Reporting Portal. This website allows citizens of India to report online crimes such as financial frauds, cyber bullying and hacking. It is an important tool for ensuring online safety and protecting citizens. The website makes it easy to file complaints about internet-related crimes. Figure 11.3 shows the homepage of the Portal. (https://cybercrime.gov.in/)

Figure 11.3 : National Cyber Crime Reporting Portal

Let us learn more about what this portal is and how it can be used.

How does it work?

- **Reporting Cyber Crimes**: If you see or experience something bad online, like a scam or someone being bullied, you can report it on the portal. It's important to tell an adult first, like a parent or teacher, and they can help you use the portal.
- **Filling out a Form**: On the portal, there is a form where you can write down what happened. You will need to include details like what kind of problem you are facing and when it happened.
- **Staying Safe**: The portal helps the government find and stop people who are doing bad things online. By reporting these problems, you help make the internet a safer place for everyone.
- **Getting Help**: Once you report a problem, the authorities can investigate and help solve the issue. They might also give advice on how to protect yourself online in the future.

The Cyber Crime Portal is important because it helps protect people from internet dangers. By reporting cyber-crimes, you help stop bad people from hurting others. It also teaches everyone about being safe online and encourages us to be responsible digital citizens.

Remember! If you ever feel unsafe online or notice something wrong, always tell to your parents and your class teacher. They can help you decide what to do next and how to use the Cyber Crime Portal. This portal is an important tool for keeping the internet safe place for everyone.

CERT-IN (Indian Computer Emergency Response Team)

CERT-IN (Indian Computer Emergency Response Team), is one of the Indian national nodal agency for responding to computer security incidents as and when they occur. CERT-In addresses threats by issuing advisories, security alerts, vulnerability notes, and guidelines to help organizations and

individuals secure their systems and networks.

For more detailed information on cybersecurity threats and best practices, you can visit the official CERT-In website: https://www.cert-in.org.in/.

Note: For additional cybersecurity practices, visit the official Cyber Crime portal of the Government of India (https://cybercrime.gov.in). The following links provide valuable resources to improve cybersecurity awareness:

- Refer a very useful document on **A Handbook for Students on Cyber Safety** at link: ***https://static.cybercrime.gov.in/Webform/Crime_OnlineSafetyTips.aspx***
- Refer important **Cyber Awareness Documents** at *link:**https://static.cybercrime.gov.in/Webform/CyberAware.aspx***

Summary

In this chapter, students are introduced to the importance of computer security in the digital age, focusing on the protection of digital resources and data privacy. It covers the fundamentals of cybersecurity, common cyber threats, basic do's and don'ts and safe browsing habits. Chapter discusses various dangers such as viruses, malware, phishing, ransomware, keyloggers, cyberbullying, and social engineering tactics. The chapter also addresses how to recognize fake websites, suspicious links, and fake SMSs. It also covers important security mechanisms, highlighting safe use of devices and applications through antivirus software and firewalls. Additionally, students are also introduced about the cybercrime portal for reporting and addressing cybercrimes, equipping them with the skills to safeguard their information online.

EXERCISE

1. Why computer security is important?
2. List the important digital resources used by Schools.
3. What do you mean by Data Privacy?
4. How to create a strong password? Give any three suitable examples of strong passwords.
5. What do you mean by a weak password? Give examples of three weak passwords.
6. Mention any three safe browsing habits for students while using the Internet.
7. Prepare a list of common cyber threats.
8. What do you mean by the Ransomware?
9. What are some safe practices to follow when downloading mobile apps?
10. Write a brief note on the secure use of Wi-Fi and the dangers of using public Wi-Fi.
11. **State whether true or false.**

    (1) Regular scans using Antivirus can protect against malware, viruses, and other cyber threats.

(2) Firewalls act as a barrier between your device and potential threats on the Internet.

(3) It is safe to reuse passwords across multiple social media accounts.

(4) Zero-day Exploits involve intercepting communications between two parties to steal data without the knowledge of legal users.

(5) Trojans are a category of malicious code that demands a payment to unlock your encrypted data.

12. Fill-in the blanks.

(1) One of the basic "do's" of cyber security is to regularly _____ your software.

(2) The _____ refer to the categories of people who aims to exploits the weaknesses of the computer system to gain unauthorised access and misuses data.

(3) A _____ password includes a mix of letters, numbers, and special characters.

(4) Antivirus software helps protect devices from _____.

(5) The Cyber Crime Portal of Govt. of India is a platform for reporting _____ activities.

13. Multi-choice questions. Choose the most correct answer.

(1) What is the primary purpose of cyber security?

(a) To improve computer speed

(b) To protect digital data from unauthorized access

(c) To increase internet bandwidth

(d) To enhance graphic quality

(2) Why is it important to follow safe browsing habits?

(a) To make your internet connection faster

(b) To avoid exposure to cyber threats and protect personal information

(c) To access more websites

(d) To improve computer graphics

(3) Which of the following cyber threats looks like legitimate software, but once activated, executes harmful actions?

(a) Virus (b) Worm (c) Trojan (d) Ransomware

(4) Which category of threats demands payment to unlock our data?

(a) Ransomware (b) Virus (c) Trojan (d) Adware

(5) Which of the following is a recommended "do" for cyber security?

(a) Use the same password for all accounts

(b) Click on pop-up ads frequently

(c) Regularly update your software

(d) Share passwords with friends

(6) What is a "don't" in basic cyber security practices?

(a) Using strong, unique passwords

(b) Sharing personal data on unsecured websites

(c) Logging out from public computers

(d) Turning on two-factor authentication

(7) Cyberbullying typically involves:

(a) Physical harm (b) Using technology to harass someone

(c) Legal action (d) Academic dishonesty

(8) Why is using a public Wi-Fi network risky?

(a) Hackers may steal our data.

(b) Clicking on such links are safe

(c) It requires a password

(d) It is more expensive

(9) Which of the following is related to a suspicious link?

(a) It has a clear, and readable URL

(b) It appears to come from a trusted source

(c) It is frequently visited

(d) Clicking on such links lead to malware download

(10) Which of the following is a type of malware?

(a) Firewall (b) Virus (c) Encryption (d) Browser

Laboratory Exercise

1. Visit the ***https://cybercrime.gov.in*** website and locate various cyber safety guidelines given under the ***Learning Corner*** section. Write a brief note on any one Cyber Safety Guideline.
2. Visit the official CERT-In website ***https://www.cert-in.org.in/*** and prepare a brief note on any three of the latest ***Security Alerts*** mentioned on the website.
3. Prepare a list of any five popular Antivirus software names.
4. Prepare a list of any five sample weak passwords. Write a justification for why they are called weak passwords.
5. Create any five Strong Passwords, and write the justification for why they are strong passwords. (Note: Don't write your real passwords in your answer.)
6. Visit various URLs and identify safe websites. Make a list of 3 safe websites.
   - Hint: Locate ***https://*** in website name
7. Prepare a security checklist for your computer:
   - **Task:** Check to ensure that antivirus software is installed, the operating system is updated, and the screen lock is enabled, etc.

8. Create a "Cyber Safety Poster".
   - Hint: Include 5 safety rules (e.g. Don't share OTP, Don't share password, etc.)
9. Create a poster on "Safe Browsing Habits for Students".
10. Prepare a poster on "Common cyber threats and its prevention mechanisms".