Cyber Safety and Security Students HandBook

Programme Coordinator

Dr. Angel Rathnabai

Central Institute of Educational Technology

National Council of Educational Research and Training

Sri Aurobindo Marg

New Delhi-110016

Acknowledgement

Programme coordinator:

Dr. Angel Rathnabai, Assistant Professor, Central Institute of Educational Technology (CIET), NCERT, New Delhi

Authors/ Module Developers:

Technical Aspect of Cyber Safety and Security:

1. Ms. Ramya Sriram, HoD Computer Science, National ICT Awardee, Campus K International School, TNHB Main Road, KTKTown, Sholinganallur, Chennai-600119
2. Ms. Anni Kumar, HoD Computer Science, National ICT Awardee, Vikas Bharati Public School, Sector 24, Rohini, Delhi-110085
3. Mr. Sandeep Arora, Vice Principal, Kendriya Vidyalaya, Old JNU Campus, NMR Delhi-110067.
4. Ms. Sangeeta Panchal, Rt. HOD Computer Science, Hansraj Model School, Punjabi Bagh Delhi, 110026

Psychological Aspect of Cyber Safety and Security:

5. Dr. Yatan Pal Singh Balhara, Professor of Psychiatry, Behavioral Addictions Clinic, AIIMS, New Delhi, 110608
6. Ms. Akanksha Rajguru, Ph.D Scholar, AIIMS, New Delhi, 110608

Physical Aspect of Cyber Safety and Security:

7. Dr. Yatan Pal Singh Balhara, Professor of Psychiatry, Behavioral Addictions Clinic, AIIMS, New Delhi, 110608
8. Ms. Akanksha Rajguru, Ph.D Scholar, AIIMS, New Delhi, 110608

Socio-Ethical Aspect of Cyber Safety and Security

9. Ms. Indu Yadav, Vice Principal, Pushp Vihar (1st Shift)
10. Mr. M. Vijayakumar, English Graduate Teacher, Govt Higher Secondary School, Somandargudim,Kallakurichi district. Tamil Nadu
11. Mr. Manoj Kumar, Principal, Mahatma Gandhi Government School 25JSN, Hanumangarh, Rajasthan, 335523.

12. Ms. Vineeta Garg, PGT Computer Science, SRDAV Public School, Dayanand Vihar, Delhi
13. Ms. Roopali Arora, PGT(Economics), Sanskriti school, Dr. S Radhakrishnan marg, Chanakyapuri, New Delhi- 110021.

Legal Aspect of Cyber Safety and Security

14. Dr. Naveen Gupta, Head of ICT Dept., St. Mark's Sr. Sec. Public School, New Delhi
15. Ms. Mohini Arora, HoD Computer Science, Air Force Golden Jubilee Institute, Subroto Park, New Delhi-110010.
16. Mr. Deepak Kumar, Deputy Commandant, I4C, MHA
17. Ms. Neeru Mittal, PGT Computer Science, SRDAV Public School, Dayanand Vihar, Delhi

Supporting Team:

1. Dr. Shahnaz Bano, Academic Consultant, CIET - NCERT, New Delhi - 110016
2. Ms. Sejal Beniwal, Junior Project Fellow, CIET - NCERT, New Delhi - 110016

Advisory Team:

1. Prof. Amarendra P Behera, Joint Director, CIET-NCERT
2. Prof. Indu Kumar, Head, DICT & TD, CIET-NCERT

Table of Content

Chapter 1: Technical Aspect of Cyber Safety and Security

1.1 Module 1: Device Safety

Objectives:

At the end of the session, learners will be able to:

- handle devices connected to the Internet
- recognize if the device is being hacked or under threat
- distinguish between secured and unsecured website
- understand the concept of Private and Public network
- downloading Applications securely
- keep communication devices healthy

Outline:

- Device Safety
- Handling devices connected to the internet
- Standard Operating Procedures for Devices used to access the cyber world
- Secured website and Unsecured website
- Steps/Practices for device health and communication safety.

1.1.1 Introduction

In the busy city of Techland, Mrinal loved all things digital. One day, his friend Arjun wanted to edit a video at his home. Mrinal suggested downloading a video editing tool, and Arjun found one on a new website. After installing it, Arjun noticed his device was slowing down a lot. His computer system was consuming internet data at a very high rate. But, on the other hand, the pages were opening very slowly and there were a few new unrecognizable icons on his computer system's desktop.

Worried, Arjun realized something was wrong with his device. Mrinal, always ready to help, decided to figure out the issue. Together, they discovered that the video editing tool Arjun installed was not good. It brought in harmful software, like a digital intruder, making Arjun's device slowdown.

To fix the issue, Mrinal showed Arjun the importance of choosing safe websites when downloading software. He explained that using well-known websites is recommended, and warned against getting tempted by quick solutions from unknown places.

To solve the problem, Mrinal helped Arjun remove the harmful software and protect his device. They added a good antivirus software to clean up any hidden threats. Mrinal also spoke about keeping the device updated and paying attention to how it works.

While fixing the device, Mrinal shared lessons about being safe online. He told Arjun to be careful and think twice before clicking on anything online.

Finally, Arjun's device became fast again, and he learned an important lesson about being safe in the digital world. This experience made them both more aware of staying safe online and keeping their device safe.

Arjun's story became a simple warning in Techland – a reminder that being safe online is crucial. Mrinal, the helpful friend, became a guide for others, showing them how to navigate the digital world with care and making sure everyone enjoyed technology without any troubles.

Choosing safe software from trusted websites is indeed an important part of keeping our devices secure. However, device safety involves more than just that. It's a broader concept that encompasses various aspects to ensure our digital devices like computer systems, laptops, smartphones, tablets etc. stay protected. Regularly updating software, installing reliable antivirus programs, using strong passwords, and being cautious about clicking on unfamiliar links are all essential components of device safety. Adopting a proactive approach, staying informed about potential threats, and cultivating responsible digital habits contributes significantly to maintaining the overall security of our devices.

1.1.2 Handling devices connected to the internet (mobile, tabs, iPads, chrome Books, etc.)

We all use the internet to access information of various kinds. At times, we use it to obtain a piece of information or, in other instances, to download software or an application. Though the internet is a vast saga of resources, each use of the Internet puts our devices at risk. Unsafe use of facilities available on the internet may harm our devices and may result in complete loss of information on the device being used to access the internet. This can happen if the software downloaded has some trojan. We will look at the word trojan a little later. For now, we may consider trojan as a hidden software, which generally tries to harm or steal your data.

Devices being used to access the internet may be harmed in the following ways :

- Slowing down in speed of the device
- Corrupting files stored in the device
- Operating system malfunction
- Excessive use of internet data, which may lead to heavy internet bills.
- Stealing of personal information and misuse at a later stage.
- Stealing of passwords stored in the system
- System used as an agent to send bulk junk emails
- System used for illegal purposes
- Locking the system and demanding money to reopen it.
- Excessive use of the internet for long hours leading to malfunctioning of the device.

The devices used to access the cyber world should be secure and well-behaved online. There is a set of Standard Operating Procedures (SOP) for devices going online, like a a rulebook for a safer digital journey.

1.1.3 SOP for Devices being used to access the cyber world

This guide introduces some easy steps to ensure your devices are secure and work properly online. By following these simple procedures, you are making sure your time in the cyber world is not just fun, but also safe and trouble-free.

- **Purchasing a device with an IMEI number**

  IMEI or International Mobile Equipment Identity is a unique number, which helps to identify a portable communication device.

  Each mobile device irrespective of its manufacture has a unique IMEI number for each of its SIM (Subscriber Identity Module) slots, i.e. if a device has two SIM slots, it will have two IMEI numbers. If your device is lost or stolen, you can use these IMEI numbers to help block your device and prevent it from being misused in any illegal activity.

  IMEI number is also helpful in knowing the brand, model, year of manufacturer, or other specifications when handling sale or purchase of old mobiles.

  Before you purchase a portable communication device, check for its IMEI number.

- **Apply proper security features when using the device for the first time**

  Before using any mobile phone, apply proper security settings to make the device more safe and secure.

  - Install proper phone lock using pattern lock pins or biometrics

- Install proper antivirus software
- Uninstall or disable bloatware (unwanted pre-installed software)
- Update all critical apps, especially your OS
- Adjust screen brightness for pleasant viewing experience.Set up mobile data tracking

- **Be careful each time the device is connected to the internet**

  Keeping a record of data usage is crucial from a security standpoint. Monitoring the amount of data consumed helps to detect any unusual or unexpected spikes in usage, which could be indicative of unauthorized access, malware, or data breaches. By regularly reviewing your data usage records, you can identify potential security threats, take prompt action to address them, and safeguard your personal information and sensitive data. Additionally, setting up data warnings and limits adds an extra layer of protection. It ensures that you get an alert and can investigate any suspicious activity before it escalates, thereby enhancing the overall security of your mobile device and data.

- **Disposing or selling off the Device**

  You should be cautious while selling a device, being used by you to access the internet. Any device that you use to access the internet contains a good amount of your personal or confidential data. This data may be in the form of personal photographs, internet use history, downloaded files, saved passwords, hint answers, etc. This data can be misused and can be used to intrude into your personal space. To avoid misuse it is recommended that you take the following precautions before you dispose of your communication or computing device:

  - Backup all your data, contacts, photographs, etc. on cloud storage or a portable device.
  - Factory reset or hard format your device before disposing of it.
  - Remove all SIM cards even if they are blocked or not in use.
  - Clean all the browsing history.
  - Remove all passwords, pattern locks, fingerprints, or face locks.
  - Wherever possible, sell your device to an authorized e-waste management firm
  - Open your Google account on another device and make sure that your account has been logged off from the device that is being disposed of.

- Keep a record of IMEI numbers if any and also of the person who takes the device.

1.1.4 Symptoms that will help to recognize if your device is being hacked or under threat

Recognizing the symptoms of a hacked device is crucial in protecting your personal information and maintaining online safety. This brief guide will outline key indicators that may suggest your device is compromised. From unusual behaviour to unexpected system changes, understanding these symptoms can empower you to take swift action and make your digital defences stronger.

- Unusual data usage
- Unusual slow processing of the device
- Unusual battery drain
- Unusual overheating of the phone
- Unexpected Pop -Ups
- Unexpected text messages or calls
- App not installed by you
- Unusual files or folders

1.1.5 Secured website and Unsecured website

1. **Secured website**

Secured websites are like reliable friends in the vast world of the internet. Think of them as trusted marketplaces where you can explore without any worries. These websites are like good shops that will not deceive/cheat you or cause any trouble. Visiting safe websites is like entering a place where everything is secure and friendly.

Similar to choosing friends wisely, it's important to pick websites that are known and trusted. These sites follow rules and do not have hidden dangers that can harm you or your device. They make your online experience enjoyable without any concerns. So, think of safe websites as your trusted companions – places that keep you protected and make sure your online journey is safe and pleasant. A secured website is an online platform that is always reliable and safe to use. In the vast landscape of the internet, distinguishing between trustworthy and potentially malicious websites is a vital skill. A keen eye and an awareness of red flags are required to identify trusted websites. This guide provides tips to assess website trustworthiness so you can confidentially navigate the digital realm.

a. **Always use the correct link to open a website or a webpage**. Always check the spelling of the link (domain name) before you open it. Usually,fake sites have very similar names to that of an original website or a page. For example, a fake website for yahoo.com may have a name like yahooo.com or yah00.com. Notice that to create a fake webpage the creator has added the letter 'o' in the name or has replaced the letter 'o' with zero.

b. **Use safe browsing tools to check if a webpage or a website linked to a URL is genuine or not.** Some tools identify whether the website contains malware, phishing scams, or other threats and alert the user before they visit them. Some tools provide safety ratings for the website based on its analysis. Examples of tools are:
Google Safe Browsing, McAfee WebAdvisor, Avast online security, etc.

c. **Check for secure connection and validity of a certificate issued to the website by an authority.** Ensure a website's trustworthiness by checking for a secure connection (HTTPS) and a valid SSL/TLS certificate.

URL begins with "https://" instead of "http://": Use websites whose URL begins with "https://" instead of "http://". To check for a secure connection, look for the padlock icon in the address bar, this indicates the encrypted data transfer.

Validity of Certificate: HTTPS checks digital certificates and ensures the authenticity of the website. A legitimate certificate, issued by recognized authorities, boosts online security and safeguards sensitive information from potential threats.

d. **Use WHOIS lookup to check for registration details of the owner and registration details of a website.** Use a Whois lookup to find out who owns a website and check its registration details. This tool tells you when the website was created, when it expires, and who registered it. Understanding this information helps you decide if a website is trustworthy. This would be like looking up a website's ID card – the more clear and accurate the details, the more you can trust it.

2. Unsecure Website

The message "**Your connection is not private**" is a browser warning that arises when there are issues with the security of a website. This message typically indicates problems with the site's SSL (Secure Socket Layer) certificate, the digital certificate that ensures a secure and encrypted connection between your browser and the web server. SSL certificates are fundamental for

protecting sensitive data, such as login credentials or personal information, from being intercepted by malicious actors.

When encountered, this error serves as a crucial precautionary measure, alerting users to potential security risks. Ignoring this warning and proceeding could expose users to various threats, including man-in-the-middle attacks, where unauthorized entities could intercept and access sensitive data during transmission.

Implications of disregarding the "Your connection is not private" warning include the potential compromise of confidential information, such as passwords or financial details. Cybercriminals may exploit vulnerabilities in the connection, leading to unauthorized access to personal accounts or the theft of sensitive data.

To address this issue, users should exercise caution and avoid entering sensitive information unless they are certain about the trustworthiness of the website. Website owners can rectify this error by ensuring their SSL certificate is valid and properly configured. Users should also be cautious when connecting to public Wi-Fi networks, as unsecured networks can increase the likelihood of encountering such security warnings and potential risks. Ultimately, understanding and responding to this error is essential for maintaining a secure online experience and safeguarding personal data from potential cyber threats.

1.1.6 Private Network and Public Network

a. **Private Network:** A private network is like a secret club for computers in a company or at home. This is a safe space where only allowed members, like computers or devices, can join. For instance, think of a company's private network, known as an intranet – like an exclusive digital meeting room where employees can share and work together securely. Similarly, at home, your private Wi-Fi network is like a virtual fortress, ensuring only your devices can connect. These networks use special passes, like passwords, to make sure only the right computers or gadgets can access them. So, just like a secret club, private networks keep things safe and sound within their digital walls, making sure only the trusted members get in.

   Some features of a private network are:

   - **Accessibility**: Limited access, typically within a specific organization or a confined physical location.

- **Ownership:** Owned and maintained by a private entity, such as a company, and used for internal communication and data sharing.
- **Security:** Generally more secure due to restricted access, making it suitable for sensitive information and confidential data.

b. **Public Network:** Public networks are like open parks where anyone can play, meaning they are accessible to everyone. Unlike private networks for specific groups, public networks are for everyone to use. However, this openness brings a challenge – they need extra safety measures. These networks are not as secure as private ones, so it's crucial to be careful. This would be like playing in a big playground; you have fun, but you also watch out for potential dangers. . So, when using public networks, one must be cautious and avoid sharing sensitive information to stay safe in the digital town square.

   Think of a public network as a busy town square in the digital world, open for everyone on the Internet. The most common one is the Internet itself, where people connect globally. Another example is public Wi-Fi found at places like Airports, Railway stations, and cafes – it's like a free digital meeting spot.

   Some features of a public network are:

   - **Accessibility**: Open and accessible to the general public or users outside a specific organization.
   - **Ownership**: Infrastructure is owned and operated by a third-party entity, like Internet Service Providers (ISPs).
   - **Security**: Less secure compared to private networks due to open access; additional security measures, such as firewalls and encryption, are necessary.

1.1.7 Secure Download of applications

Ensure you download apps safely to protect your device and personal information. This guide will help you understand why it is crucial to get apps only from trusted sources , check what they are allowed to do, and use good security software. The following simple steps can help keep your device safe from bad apps and ensure your information stays private.

- **Always use trusted sources to download an app or software**. Trusted sources include the official websites of software, web-stores of reputed companies like Google, Microsoft, Apple, etc.

- **Avoid downloading software or apps from torrent clients** as these services provide downloads from untrusted sources.
- **Check for the rating or reviews of the software or the app being downloaded.** Look for reviews or testimonials on the official website or from reputable sources. Positive feedback from other users is a good indicator of reliability.
- **Review permission required by applications.** Before downloading an app, review the permission it requires. Avoid downloading if it requires unwanted permission.
- **Verify System Requirements:** Confirm that your device meets the software or app's system requirements. This information is usually available on the official website.
- **Avoid Third-Party Websites**: Refrain from downloading software from third-party websites. Stick to official sources to minimize the risk of downloading compromised versions.
- **Check for Digital Signatures:** Some software developers provide digital signatures to verify the authenticity of their files. Check for this information on the official website.

1.1.8 Steps/Practices for device health and communication safety.

We use our communication devices very frequently for personal and professional use. Most communication happens through devices these days. So it becomes important to take care of devices so that the data stored in our devices is not vulnerable to any cyberattack. It is very important to keep communication devices healthy. These are the few steps that help to manage the device's health.

Ensuring the health of your communication device is essential for optimal performance and longevity. This brief guide outlines key practices to keep your device in top shape. From regular updates and efficient storage management to responsible usage habits, adopting these measures contributes to a smooth and secure communication experience. Let us explore simple steps to maintain the health of the communication device and enhance its overall functionality.

- **Avoid Unwanted Apps:** Only download essential apps to maintain a clutter-free device, ensuring smoother operation and preventing unnecessary data usage.
- **Regular App Updates:** Keep your apps up to date for access to new features, improved performance, and crucial security enhancements, ensuring a seamless and secure user experience.

- **Uninstall Unused Apps:** Free up valuable storage space and streamline your device by removing apps that are no longer in use, optimizing its overall performance.
- **Turn Off Connectivity:** When not in use, deactivate Bluetooth, Wi-Fi, or hotspot features to conserve battery life, enhance privacy, and minimize the risk of unauthorized access to your device.
- **Use the Correct Charger:** Safeguard your device's battery health by using the correct charger and cable, avoiding loose or malfunctioning power sockets that could potentially damage your device.
- **Avoid Overcharging:** Prevent long-term battery issues by disconnecting your device once it is fully charged, ensuring optimal battery life and efficient power usage.
- **Replace Battery Timely:** Keep your device running smoothly by replacing the battery when its lifespan is over, preventing potential issues and maintaining overall performance.
- **Sunlight Exposure:** Shield your device from direct sunlight to prevent overheating, damage to internal components, and potential performance issues.
- **Optimal Brightness:** Adjust your device's screen brightness to a comfortable level, preserving battery life and reducing eye strain.
- **Handle Heating Issues:** If your device becomes excessively hot or processes slowly, power it off temporarily to avoid potential damage and allow it to cool down.
- **Quality Screen Guards:** Invest in high-quality screen guards and back covers to protect your device from scratches, impacts, and everyday wear and tear, ensuring its longevity.
- **Avoid Device Sharing:** Maintain the security of your personal data and settings by refraining from sharing your devices, reducing the risk of unauthorized access and potential privacy breaches.

1.1.9 Do’s and Don’ts

To summarize here are some Do’s and Don’ts for internet-connected devices:

Do:

- **Keep Software Updated:** Regularly update your device's operating system and applications to patch security vulnerabilities.

- **Use Strong Passwords**: Create strong, unique passwords for your accounts to prevent unauthorized access.
- **Enable Two-Factor Authentication**: Add an extra layer of security by enabling two-factor authentication whenever possible.
- **Install Reliable Security Software**: Use reputed antivirus and anti-malware software to protect against online threats.
- **Encrypt Your Device:** Enable device encryption to safeguard your data in case of theft or loss.

Don't:

- **Ignore Software Updates**: Always install the latest updates to benefit from security fixes and improvements.
- **Share Sensitive Information Insecurely**: Avoid sharing personal or financial information on unsecured websites or public networks.
- **Click on Suspicious Links:** Be cautious of unsolicited emails or messages and avoid clicking on links from unknown sources.
- **Use Weak Passwords:** Steer clear of easily guessable passwords; opt for a mix of letters, numbers, and symbols.
- **Download Apps from Untrusted Sources:** Only download apps from official app stores to minimize the risk of malware and security breaches.

By adhering to these do’s and don'ts, you enhance the security of your internet-connected devices and protect your personal information from potential cyber threats.

1.2 Module 2: Browser Safety

Objectives:

At the end of the session, learners will be able to:

- Importance of browser features and functionalities.
- Choose appropriate privacy and security settings in the browser.
- Adopt safety measures while browsing.

Outline:

- Browsers
- Browser interface.
- Uniform Resource Locator
- Regular browsing and private browsing
- Browser History
- Firewall
- Cookies
- Website Privacy preferences
- Identifying fake websites
- Browser safety measures

1.2.1 Introduction

If you want to access information from a book in the library, what would you do? You would take the help of the librarian, who would fetch the book for you. Similarly, when you want to access information in the digital world, you need software that can fetch information for you in the form of web pages/websites. That software is called a web browser. Just as a librarian helps you find and handle books in the library , the browser helps you open and access websites on the internet.

1.2.2 Web Browser

A web browser is a software application that allows users to access and interact with information on the World Wide Web. It serves as a gateway between users and the vast expanse of online content, enabling them to view web pages, download files, and engage in various online activities.

Many web browsers are available. Common web browsers are:

- **Google Chrome-** Developed by Google, Chrome is one of the most popular browsers known for its speed, simplicity, and smooth integration with other Google services.
- **Mozilla Firefox-**is an open-source browser that prioritizes privacy and user control. Firefox has a strong emphasis on customization through add-ons(programs that can be added to a main program to improve its performance) and offers strong privacy features like Enhanced Tracking Protection.

- **Microsoft Edge-**Developed by Microsoft, Edge replaced Internet Explorer and is based on the Chromium engine (the same engine as Chrome). It boasts a clean interface, integration with Microsoft services, and performance improvements.
- **Apple Safari-**is the default browser for Apple devices, and is known for its speed and energy efficiency. It is tightly integrated with the macOS and iOS ecosystems and features various privacy-focused tools.
- **Opera-**is a feature-rich browser known for its built-in ad-blocker, free VPN, and customizable interface. It aims to provide a fast and secure browsing experience with unique features.
- **Brave-**is a privacy-focused browser built on Chromium, Brave blocks ads and trackers by default. It also has a unique model where users can opt to view privacy-respecting ads in exchange for rewards.
- **Vivaldi-**is designed for power users who appreciate customization. It offers extensive settings, tab management, and a visually appealing interface, making it stand out among browsers.

Each browser mentioned has its strengths and weaknesses. Catering to different user preferences, users can choose a browser based on factors such as speed, security, privacy features, and integration with other services. Browsers play a crucial role in shaping the internet experience, and their functionalities have evolved over the years.

Before we understand the various functionalities of the browser, let us understand its interface.

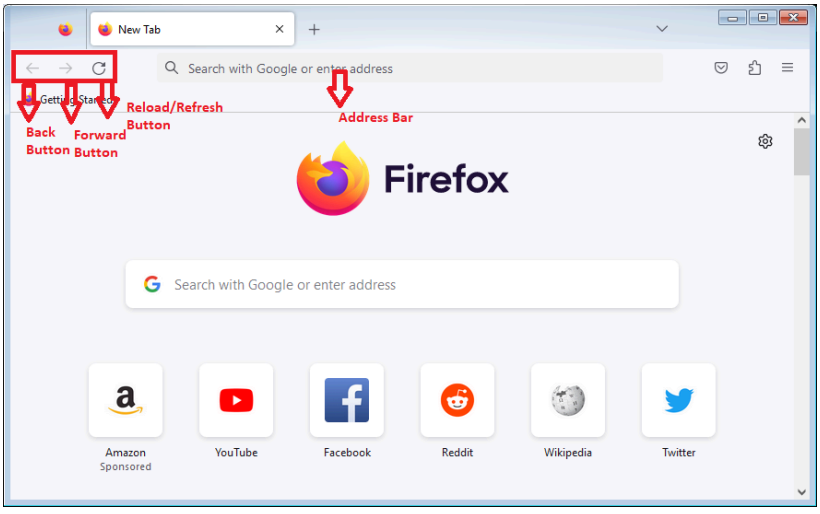


Figure 1: Firefox

- **Back button:** It helps us to go back to the webpage previously visited. It is like turning back a page in the book.
- **Forward button:** it helps us to move forward to a page we previously visited after using the back button.
- **Reload/refresh button**: It reloads the current webpage. It is helpful if the page is not loading properly or if we want to see any updates on the webpage.
- **Home button:** It takes us to the browser's web page, which we can set to our preferred website.
- **Address bar:** We can type the address of the website we want to visit in the address bar.
- **Tabs**: These are like different pages in a book. We can have multiple tabs open at once, each displaying a different webpage, which helps in multitasking and easy navigation between websites.

As discussed earlier, the primary function of a browser is to retrieve and display web pages. But how do we know where the webpages are located? Imagine you want to visit your friend's house. The first thing you need is your friend's house address. Similarly, every web page on the internet has an address. We call it the URL, Uniform Resource Locator. This URL helps to identify the webpage on the World Wide Web. When a user enters a web address/URL in the address bar, the browser fetches the relevant web page and displays the webpage on our screen.

Imagine you are reading a book, and you want to mark a specific page that you want to return to later without having to remember the page number. In that case, we use a bookmark. Similarly, if we want to revisit a webpage later, we can bookmark the webpage for future reference. This allows us to save and revisit our favourite websites. Browser helps us to access web pages along with many functionalities. While accessing web pages using a browser, we need to ensure we follow all safety protocols so that we can stay safe online.

1.2.3 Safety features in Browser

Assume you have some internet connectivity issue or the computer at your home is not working, and you need to submit an assignment to your teacher through email, and today is the last day for submission. How to handle this situation? You can go to the browsing centre and send the email. But when you login to your email account on a computer which is accessed by many random people, there are chances of compromising safety of your account. To avoid this, you can use an incognito tab in your browser and keep the browsing details private.

1.2.3.1 Using a Private tab

Using a Private tab is simple! Here are the steps:

- Launch your web browser. This could be Chrome, Firefox, Safari, or any other browser.
- Look for three dots in the upper right corner in Chrome, three horizontal lines on the top-right corner (Application Menu) in Firefox, or an icon with the word "File" in Safari. Click on it.
- In the menu that appears, you will see an option like "New Incognito Tab" in Chrome, "New Private Window" in Firefox, or "Private Window" in Safari. Click on it.

  Let's take the example of the Firefox browser.

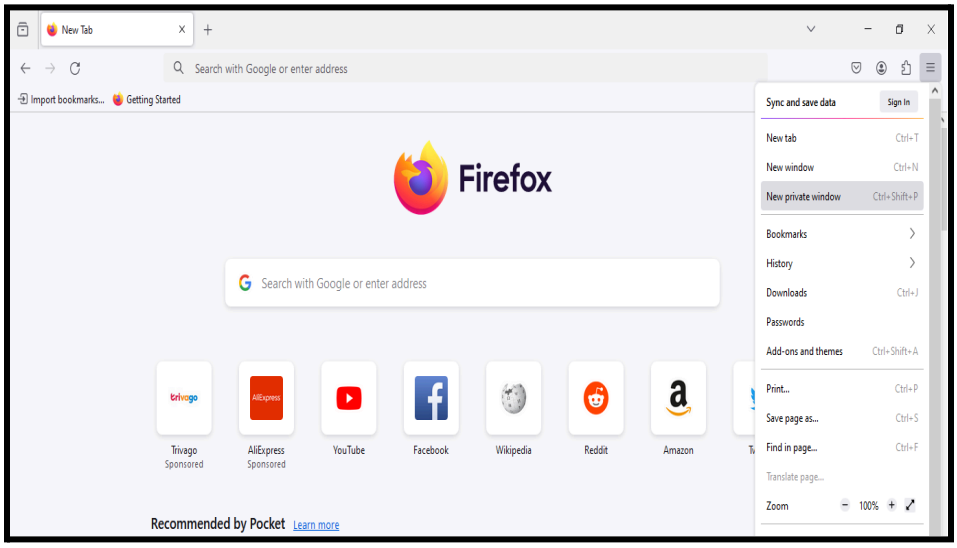


Figure 2: Firefox browser

- A new window or tab will open in incognito mode. The darker theme or symbol indicates that you are incognito. Now you can browse privately.

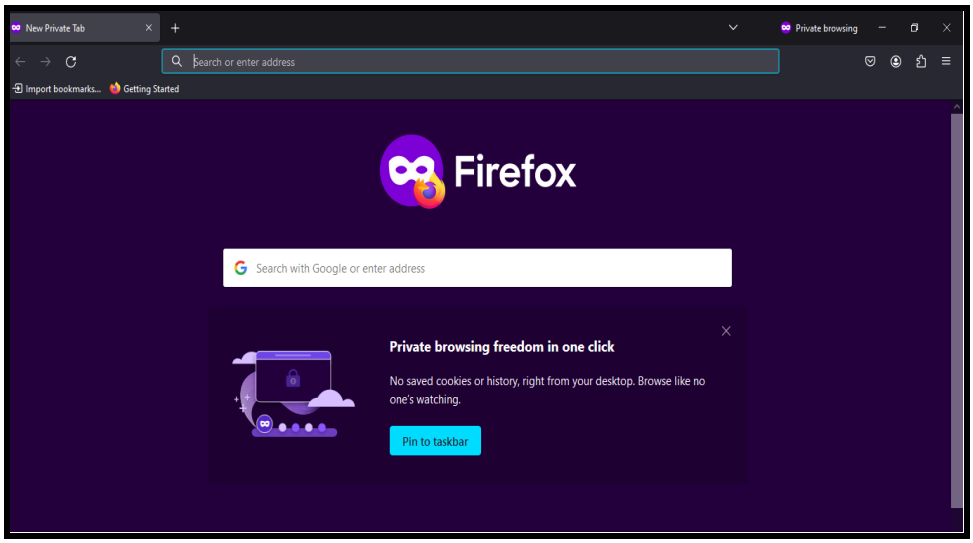


Figure 3: Incognito Mode

- When you are done with your incognito session, close the tab or window. This ensures that your private session is ended, and no history or cookies are saved.

Using a private/incognito window ensures all the browsing activities get deleted once you close the tab. So any other person using the same computer, will not be able to track your browsing details as it does not keep record of the websites visited.

Incognito also provides personal space for your online activities. Incognito tabs do not mix with the regular tabs, so you can log into multiple accounts simultaneously without worrying about one messing with the other. This is like having your own private corner on the internet. Incognito mode does not play memory games with your usernames and passwords. In regular tabs, your browser might remember them for convenience. But an incognito tab is like having a digital vault that does not save your sensitive information.

Let's assume that after going to the browsing centre, you forget to open the incognito window and start using the regular window in the browser. You remember about this later when you have completed your browsing. In this case, you can go to 'History' of your browser and delete all the websites that you visited, so there is no trace of your browsing activity. Let's see how we can do it.

- Open Mozilla Firefox browser and click on the 'Application Menu' and Click 'History'.

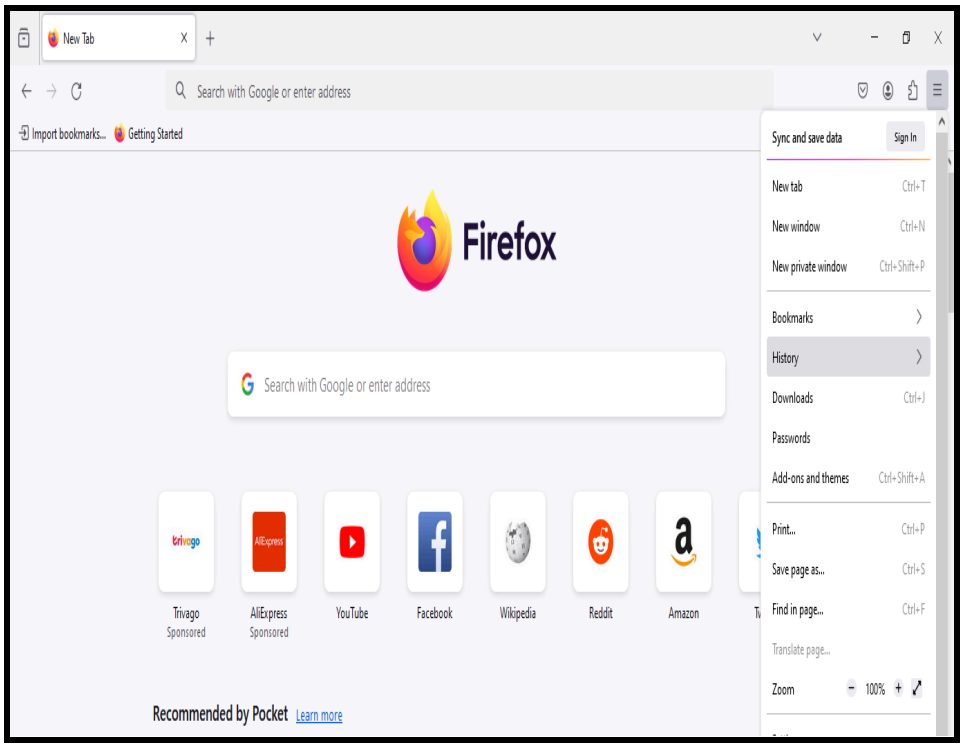


Figure 4: 'Application Menu'

Click 'Clear recent history'.

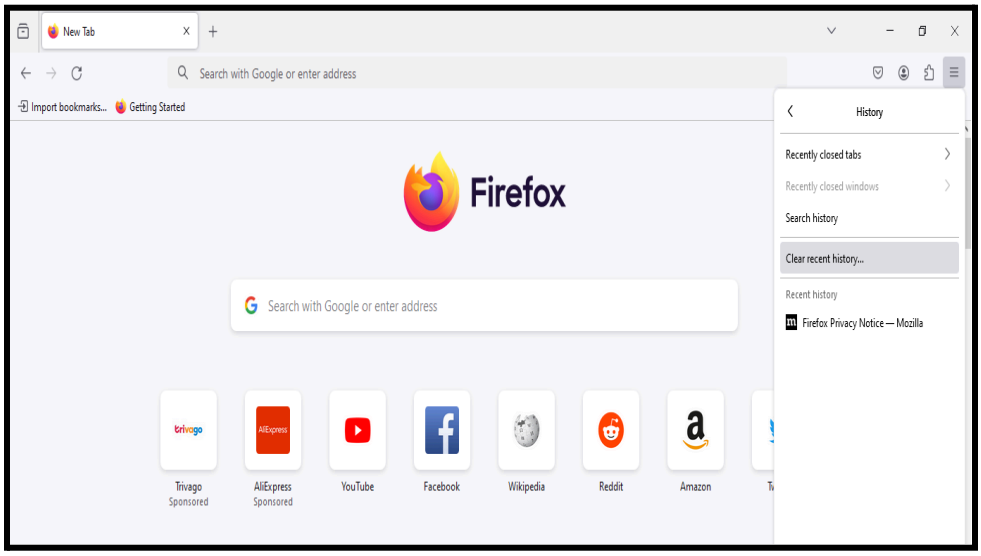


Figure 5: 'Clear recent history'

The 'Clear recent history' dialogue box appears. Choose the time range and the data you want to delete and 'Clear Now' button.

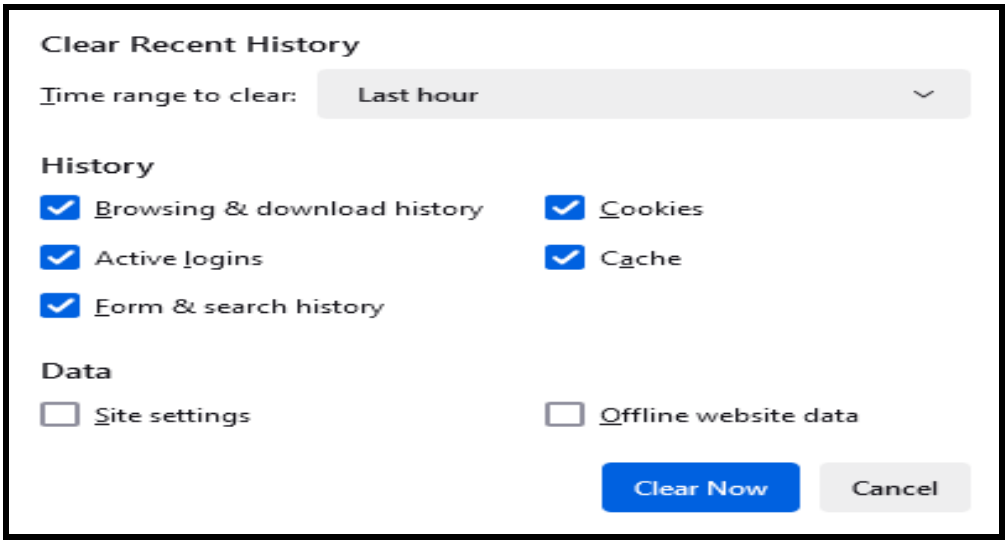


Figure 6: 'Clear recent history'

This deletes all your browsing history and ensures safe browsing when you use shared computers in the browsing centre or in your school lab.

You can also go to 'Settings' from 'Application Menu' and choose 'Privacy & Security'. Scroll down to 'History' and click the 'Clear History' button. You can also set whether you want the browser to always remember history or never remember history or do custom setting for history.

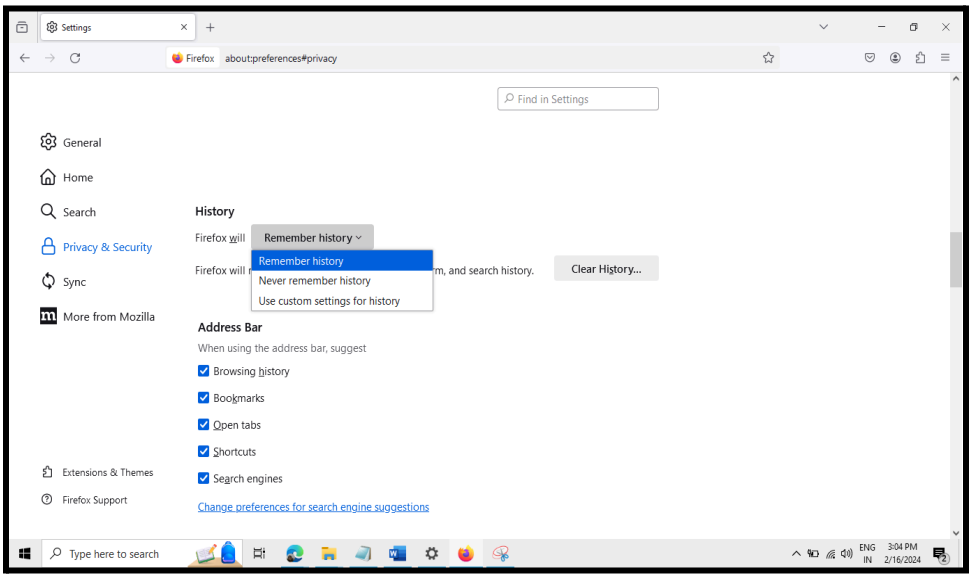


Figure 7: 'History'

1.2.3.2 Firewall

Let us consider another scenario. When checking email, you received an email from an unknown account and clicked on the link sent in the mail. After clicking, your computer became

slow and glitchy You worried and asked your friend, Rohan to check it up. Rohan figured out the issue and had a simple solution – a firewall. The firewall is like a shield for the computer, functioning like a sort of digital security guard. It checks all information before letting in, making sure that only reliable information enters.. In simple terms, a firewall is a software that watches over the digital traffic, ensuring that no unauthorized person gains access to the network, and thus keeps you safe on the internet. You can block dangerous content in your browser 'Privacy & Security' setting as shown below.

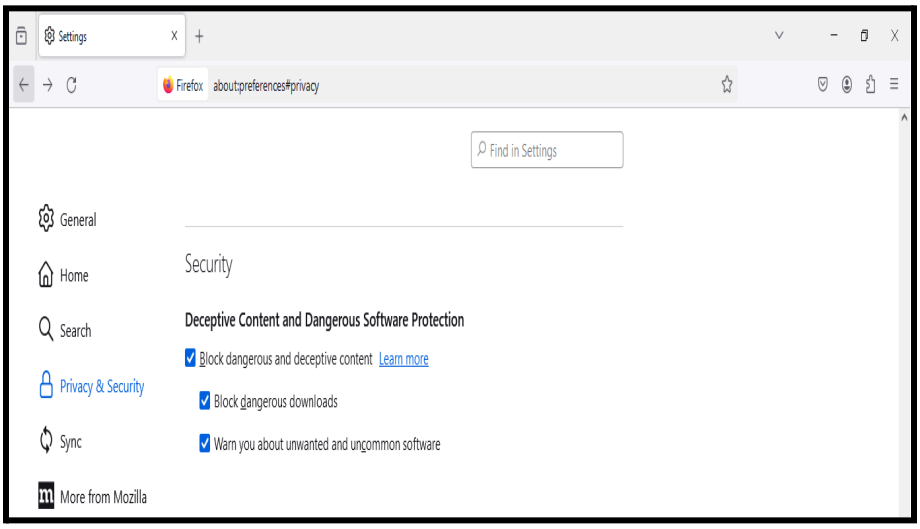


Figure 8: Privacy & Security

How Does a Firewall Work?: It watches over the traffic between your computer and the internet. In case of suspicious behaviour, the firewall blocks entry. . This is It's like having a guard at the gate who only lets in the good people (authorized person).

Uses of a Firewall

- **Blocking Online Bullies**: Sometimes, digital bullies try to mess with your computer by slowing it down. The firewall steps in and says, "No bullying allowed here!" to keep your computer running smoothly.
- **Stops websites from accessing your digital data**: When you are on the internet, websites might want to know more about you. The firewall helps you stay a bit mysterious. It hides some of your digital data, making it harder for websites to follow your every move.

- **Safe Online Shopping**: If you shop online and worry about sharing your credit card details or OTP, the firewall is like an extra lock. It checks if the website is safe, making sure your money information stays safe from digital pickpockets.
- **Helping Parents Keep an Eye**: The internet is not always a safe place for children. The firewall helps parents ensure that their children only visit age-appropriate websites

1.2.3.3 Cookies

Imagine you are attending a party at your friend's house. When you arrive, your friend gives you a sticker with your name on it. Let's assume this sticker helps the organizer of the event remember who you are and what you do and like throughout the party. Similarly, when you enter the online world, you get a digital sticker called cookie. When you visit a website for the first time, it gives your web browser a small piece of information called cookie, which gets stored in your computer.

Let's assume that you are shopping online for a pair of shoes. You visit an online shoe store and browse through the selection. As you are looking, you add a few pairs of shoes to the shopping cart but decide not to purchase anything right away. The website uses cookies to remember the items you have added to the cart. After closing the website, if you visit again later, the website can still remember the items added in your cart. This makes it convenient for you to pick up from where you left off without having to start over. The cookie contains information about your visit such as your preferences, login details or items you have added to the shopping cart. Just like the sticker helps the organizer remember your preferences at the birthday party, the cookie remembers your preferences, username, shopping cart contents etc.

In Mozilla Firefox browser, Click 'Application menu' and click 'Settings'. Choose 'Privacy and Security' and scroll down for 'Cookies and Site Data'. Click 'Clear Data' button.

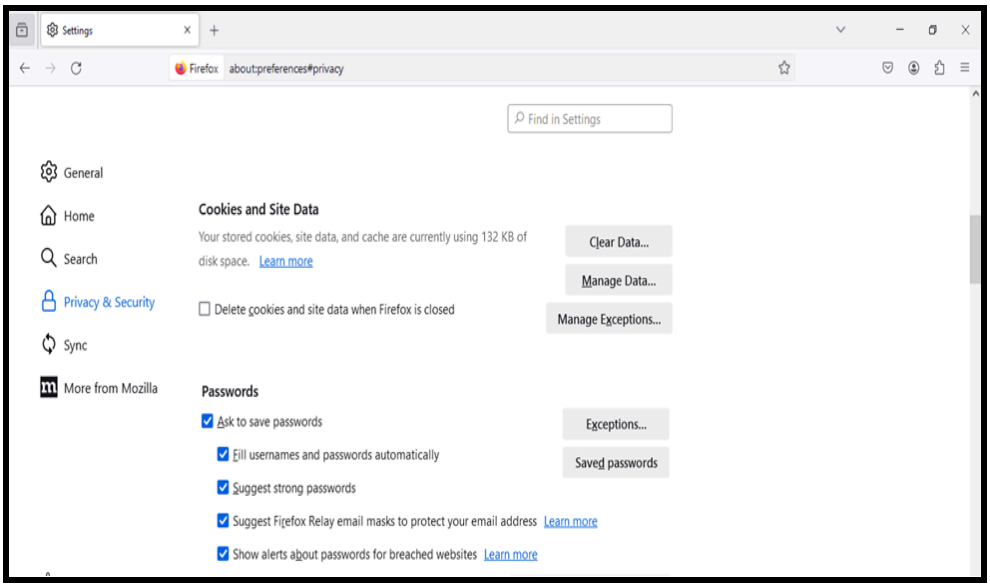


Figure 9: Cookies and Site Data

'Clear Data' dialogue box appears and check the boxes for which you want to delete the data and click 'Clear' button.

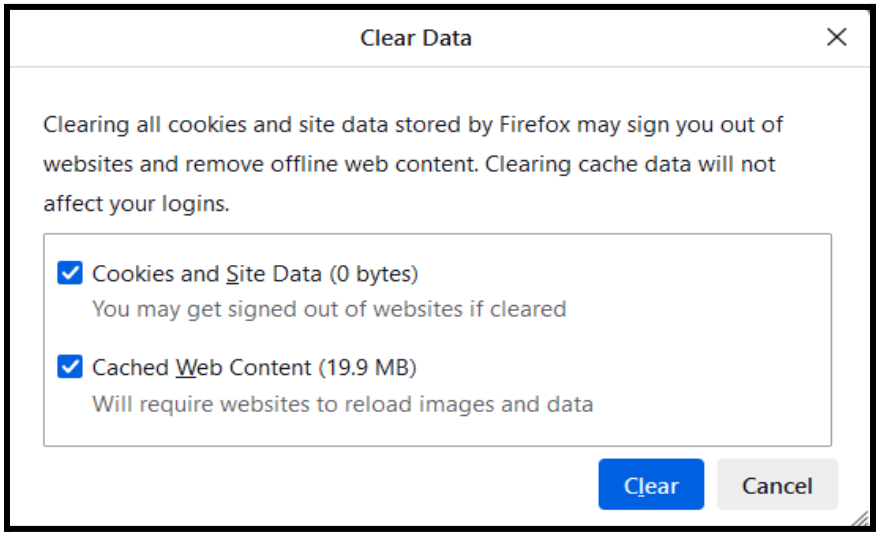


Figure 10: Clear Data

The cookies will get deleted, leaving no traces of your browsing preferences.

The trackers follow you around online to collect information about your browsing habits and interests. Firefox blocks many of these trackers and other malicious scripts.

In the browser 'Privacy and Security', you can choose to set the tracking protection to

i) Standard : Balanced for protection and performance. Pages will load normally.

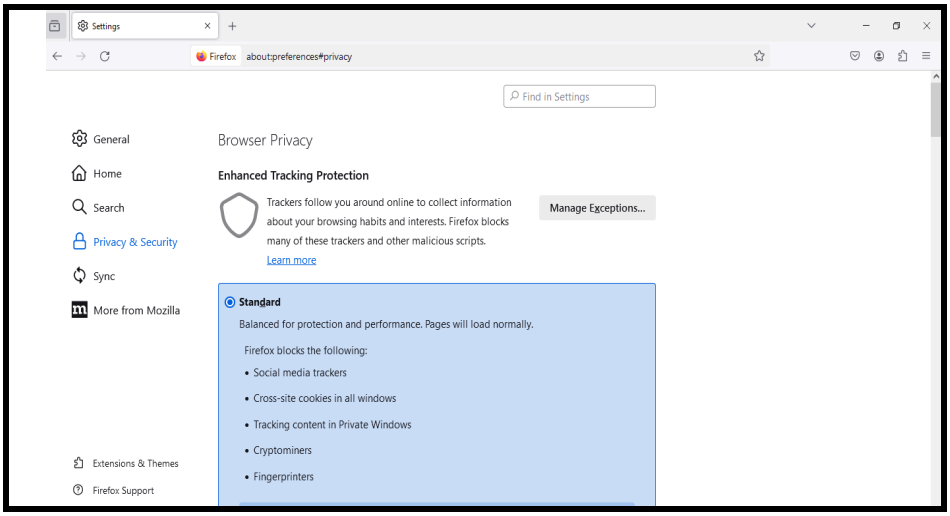


Figure 11: Tracker

ii) Strict: Stronger protection, but may cause some sites or content to break.

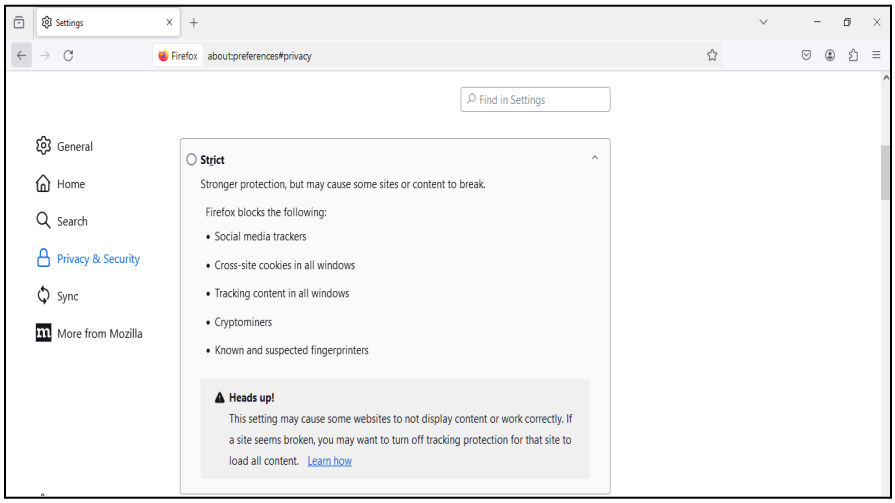


Figure 12: Privacy and Security

iii) Custom: Choose which trackers and scripts to block.In ‘Privacy and Security’, you can also set the website Privacy preferences as shown below.

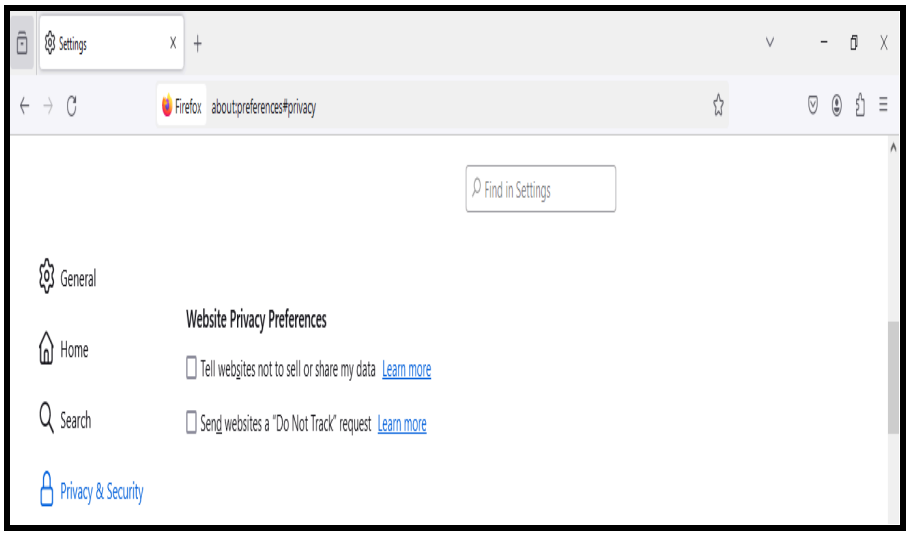


Figure 13: Website Privacy Preferences

You can also specify which websites can access your location, Camera, Microphone, speaker etc. in the 'Permissions' section of 'Privacy & Security' in the browser. You can also block new requests asking to access your information.

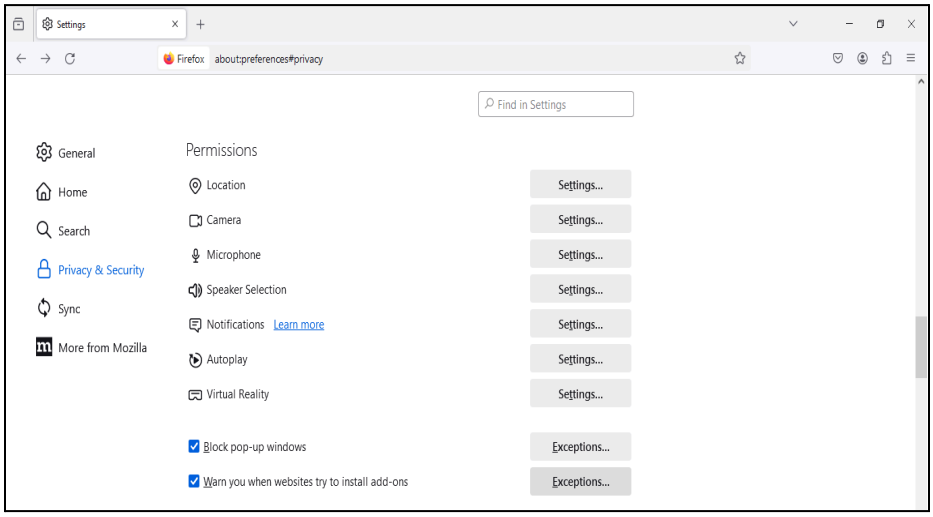


Figure 14: Permissions

Click on the 'Settings' button beside each option and enter the website URL and click 'Save Changes' button. You can check the box to block new requests asking to access your information.

You can also block pop-up windows while browsing and get alerts when websites try to install add-ons as shown below to stay safe while browsing.

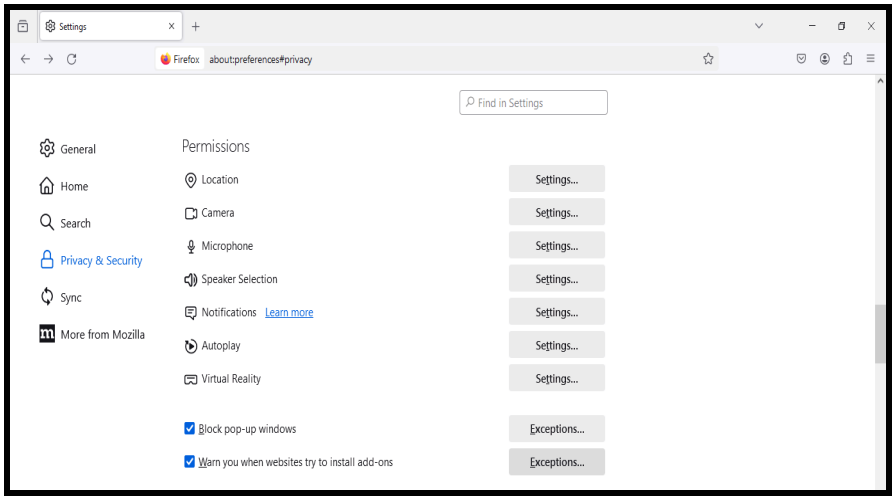


Figure 15: Block Pop-up Windows

1.2.4 Fake websites and their recognizability

Fake websites are like digital pretenders, pretending to be real but aiming to fool you. They might ask for personal info, sell fake products, or spread lies. Look out for weird web addresses, spelling mistakes, or deals that sound too amazing. Stick to trusted sites and double-check before sharing details or making purchases online. Stay smart and keep your online adventures safe!

Recognizing fake websites is crucial in today's digital age, where online scams and fraudulent activities abound. Here's a guide with examples to help you navigate the online landscape and stay safe from deceptive websites.

1.2.4.1 Understanding the Basics

Before diving into specific signs of fake websites, let's understand some general concepts:

- **Check the URL**: The website's address or URL is a crucial clue. Legitimate websites often have simple and clear URLs. Be aware of URLs with misspellings, extra characters, or unusual domain names.
- **Look for HTTPS:** Legitimate websites use HTTPS (Hypertext Transfer Protocol Secure) for secure communication. Check for the padlock symbol in the address bar, indicating a secure connection. Fake websites might lack this security feature.

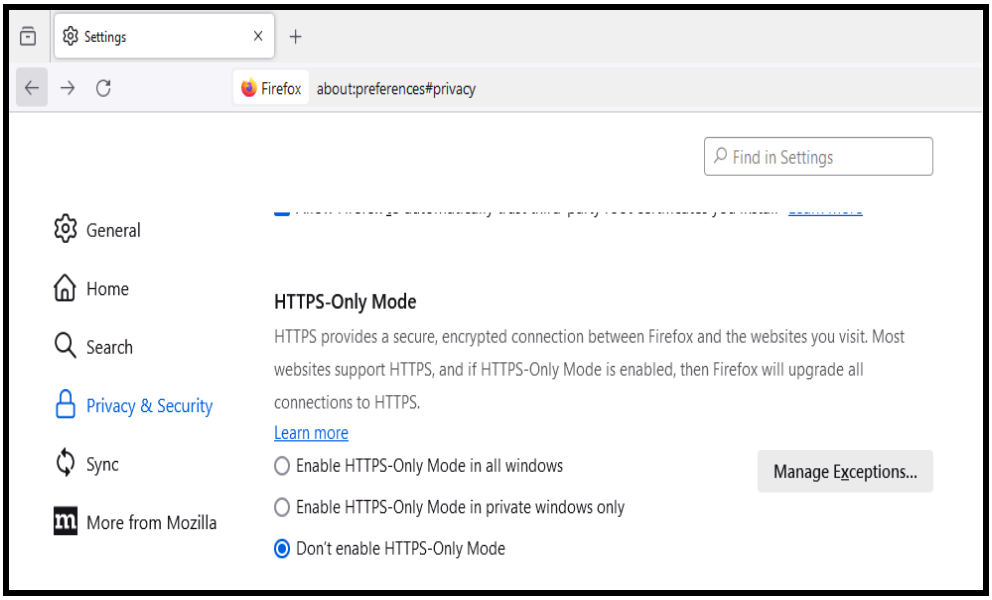


Figure 16: HTTPS

- Go to 'Privacy & Security' setting, ensure that 'Don't enable HTTPS-Only Mode' is ON. If any of the other two options is selected, then the browser will upgrade all connections to HTTPS.
- **Verify Contact Information**: Legitimate websites provide clear and accessible contact information. Fake ones may have vague or missing contact details. Be cautious if the only way to contact the site is through a form or email without a physical address or phone number.

1.2.4.2 Signs of a Fake Website

- **Poor Website Design:** Real websites invest in professional designs. If a website looks poorly designed, with low-quality graphics, misspellings, or broken links, it may be a red flag. Scammers generally do not prioritize the visual aspects of their fake sites. *Example:* A fake online store with pixelated images, awkward layout, and spelling errors in product descriptions.
- **Too Good to Be True Deals**: Fake websites often lure users with unbelievable offers, discounts, or products. If a deal seems too good to be true, it probably is. Scammers use enticing offers to attract visitors and trick them into providing personal information or making purchases. *Example:* A website claiming to sell high-cost gadgets at lower prices, aiming to tempt unsuspecting shoppers.

- **Lack of Contact Information**: Legitimate businesses want customers to reach out to them. If a website lacks proper contact information or provides only a generic email address, be cautious. Scammers aim to avoid communication that may expose their fraudulent activities. *Example:* A website selling products without any customer support contact details or a physical address.
- **Suspicious Domain Names**: Fake websites often have domain names that imitate well-known brands or use slight variations to deceive visitors. Pay attention to misspellings, extra characters, or odd domain extensions. *Example:* A fraudulent site using "amazon-sale-discounts.com" instead of the authentic "amazon.com."
- **Check the About Us Page**: Legitimate websites usually have an "About Us" page providing information about the company, its history, and its mission. Fake websites may have vague or entirely missing 'About Us" pages. *Example:* A website claiming to be an established company but lacking details about its history, team, or mission.
- **Grammar and Spelling Mistakes**: Legitimate businesses strive for professionalism, including proper grammar and spelling. Fake websites often have noticeable errors in their content. *Example:* A phishing site with emails or product descriptions containing grammatical mistakes or awkward language use.
- **No Privacy Policy or Terms of Service**: Genuine websites have clear privacy policies and terms of service, outlining how they handle user data and the rules users must follow. Fake websites may lack these essential documents. *Example:* A website asking for personal information without providing a privacy policy or terms of service.
- **Verify Online Reviews**: Real customer reviews can provide insights into a website's legitimacy. Be cautious if a site has no reviews or if all reviews seem overly positive. Scammers may create fake reviews to appear trustworthy. *Example:* A website with only a few, highly positive reviews that seem generic or fabricated.
- **Watch for Pop-Up Ads and Redirects**: Legitimate websites seldom bombard users with excessive pop-ups or unexpected redirects. Fake sites often use these tactics to push unwanted advertisements or malware. *Example:* A website displaying numerous pop-ups urging users to click on suspicious links or download unwanted software.
- **Trust Your Instincts**: Sometimes, your gut feeling is a reliable indicator. If something feels off or too good to be true, take a step back. Trust your instincts and investigate

further. *Example:* A website creates a sense of urgency, pressuring users to make immediate decisions or provide sensitive information.

Being able to recognize fake websites is an important skill in today's online environment. By staying vigilant and paying attention to the signs mentioned above, you can protect yourself from scams, phishing attempts, and other fraudulent activities. Always take the time to verify the originality of a website before providing personal information or making any transactions. Remember, a little caution goes a long way in ensuring a safe and secure online experience.

On the internet, there are good and tricky places. Web browsers, like Google Chrome or Safari, help you explore by opening web pages. They have tools, like bookmarks and tabs, to make it easy.

Imagine the incognito tab as a secret room for your online stuff. It doesn't remember where you go, perfect for surprises or private searches. It's like your online superhero, keeping things hush-hush.

Firewalls act like digital guards. They check who is trying to enter your computer, letting in good things and blocking the bad. It's like a shield for your computer.

Cloud storage is like a magical backpack in the sky. It keeps your drawings, videos, and special things safe. You can access them from anywhere, like a digital treasure chest.

In the same manner, , there are good and bad websites. Look out for bad ones pretending to be real. Check if the website's address is spelled right. If a deal seems too amazing, it might be tricky. Remember, use incognito for secrets, let firewalls guard your computer, keep your digital stuff in the cloud backpack, and watch out for tricky websites. Stay safe and have fun exploring the internet!

Ensuring browser safety is essential for protecting your online privacy and security.

Keep your browser updated: Regularly update your browser to the latest version. Browser updates often include security features that address vulnerabilities.

Install security extensions: Use reputable browser extensions or add-ons specifically designed to enhance security, such as ad blockers. Use of https forces websites to use encrypted connections wherever available.

Use a reputable browser: Choose a browser known for its security features and regular updates, such as Google Chrome, Mozilla Firefox or Microsoft Edge.

Enable automatic updates: Configure browser settings to automatically update to the latest version. This ensures protection against the latest security threats.

Enable phishing and malware protection: Modern browsers offer built-in features to detect and block phishing attempts and malicious websites. Enabling these features in the browser settings provides online security.

Use strong and unique passwords: Use a password manager to generate and store complex, unique passwords for each website. This prevents unauthorised access to the accounts even if one password is compromised.

Privacy settings in the browser: Use the browser's privacy settings according to the requirement. Disable features that compromise your privacy, such as location-tracking or third-party cookies.

Clear browsing data: Remove history, cookies and cached files to delete potentially sensitive information stored in the browser.

Following the above steps periodically will help you to be safe while browsing the web.

1.3 Module 3: Data Safety

Objectives:

At the end of the session, learners will be able to:

- understand the importance of data safety in today's digital era.
- explore the challenges and risks associated with safeguarding sensitive information.
- analyze real-world scenarios, and illustrate the consequences of data breaches and the importance of proactive measures.
- understand various data safety devices and strategies, including malware protection, antivirus software, phishing awareness, and password management.
- provide insights into the types of malware, their characteristics, and the preventive measures to mitigate their impact.

- examine the role of antivirus software in defending against malware and maintaining a secure computing environment.
- discuss common antivirus programs used for both computers and mobile devices and their key features.
- elucidate the significance of regularly updating virus definitions to combat evolving cyber threats.
- raise awareness about phishing emails, and best practices for identifying and avoiding them.
- outline the fundamentals of creating strong passwords, implementing multi-factor authentication, and adopting secure password storage practices.
- emphasize the importance of user education, access restrictions, and proactive monitoring in enhancing data safety.
- provide recommendations for establishing robust standard operating procedures (SOPs) for dealing with passwords and ensuring continuous improvement in cybersecurity measures.

Outline:

- Introduction to Data Safety
- Understanding Malware
- Role of Antivirus software and commonly used Antivirus software
- Significance of updating virus definition
- Understanding Phishing Emails
- Password security best practices
- Enhancing data security features

1.3.1 Introduction

Data safety is of paramount importance in our increasingly digital world, where vast amounts of information are generated, stored, and exchanged every day. With the pivotal role that data plays in businesses, government operations, and personal lives, safeguarding it against unauthorized access, loss, or corruption has become a critical concern. In this digital landscape, individuals and organizations alike must adopt robust measures and practices to ensure the security and integrity of their data.

Data safety is crucial in our digital age, safeguarding sensitive information from unauthorized access or loss. As data usage grows in importance across various sectors, ensuring its protection is paramount.

Let's delve into the notion of safeguarding data by looking at the experience of Geeta. Geeta, a diligent woman, was employed at a prominent financial institution aiding individuals with their finances. Unfortunately, one day, the company fell victim to a cyberattack perpetrated by malicious individuals. As a result, vast amounts of personal and financial data belonging to the company's clients were compromised. This incident led to significant chaos; clients suffered financial losses, experienced identity theft, and the company's reputation was severely tarnished.

Geeta was responsible for ensuring the security of all the information, and she approached this task with great diligence. Employing sophisticated encryption methods, she meticulously monitored the data regularly to ensure its safety. However, despite her efforts, the malicious actors managed to bypass her safeguards. This served as a wake-up call for Geeta, highlighting the ever-evolving nature of cyber threats and the need for continual innovation in information protection strategies.

Determined to rectify the situation, Geeta took proactive measures. She upgraded the company's security measures, implementing more robust safeguards and imparting comprehensive training to all employees on exercising heightened caution. Additionally, she established an emergency response team ready to swiftly address any future breaches. Geeta also engaged with experts in the field, exchanging insights and knowledge to bolster their collective defence against cyber threats.

The story of Geeta underscores the critical importance of safeguarding information, particularly in today's digital landscape. It emphasizes the necessity for individuals to educate themselves on essential security practices such as password management, configuring privacy settings, and exercising vigilance online. By staying conscious and informed, we can shield ourselves and others from the perils of cyberattacks.

1.3.2 Malware

Despite Geeta's constant vigilance, she could not figure out how her computer got infected. Upon reflection, she remembered an incident when she received an email from an unfamiliar sender while working on her computer. Initially harmless-looking, the email led her to click on a link,

triggering strange behaviour on her computer. Unbeknownst to her, this seemingly innocent email contained malware – malicious software designed to damage computers or steal data.

As Geeta continued her work, she noticed her computer slowing down and encountering unusual pop-up messages. Recognizing the signs of trouble, she promptly reported it to the IT department. Upon investigation, they confirmed that malware had infiltrated Geeta's computer, jeopardizing not only her data but also the company's information.

The malware behaved like a stealthy thief lurking within Geeta's computer, attempting to pilfer valuable information or disrupt her work. Fortunately, with the assistance of the IT team, they eradicated the malware and fortified the company's defences against future threats. Geeta learned a valuable lesson about exercising caution with emails and websites to avoid falling prey to malware.

Just as illustrated in Geeta's experience, malware poses a significant threat to our computers and personal data. It's crucial to remain vigilant and think twice before clicking on suspicious links or downloading unfamiliar files. By staying informed and employing antivirus software, we can safeguard ourselves against malware and maintain the security of our digital assets.

Malware, a short form for malicious software, is a broad term encompassing various types of software intentionally designed to harm, exploit, or compromise computer systems, networks, and user data. This software is created with malicious intent, often for financial gain, theft of sensitive information, or disruption of normal computer operations.

Malware comes in various forms, each with specific functions. Viruses replicate by attaching to legitimate programs, worms spread independently across networks, and Trojans masquerade as legitimate software to carry out malicious tasks. Ransomware, a prevalent type, encrypts files and demands payment for decryption, causing widespread financial losses and disruptions.

Malware is often spread through deceptive methods, such as phishing emails, infected websites, or malicious downloads. Cybercriminals continuously evolve their tactics, making it challenging to stay ahead of potential threats. The consequences of a malware infection can range from data breaches and financial loss to system crashes and compromised privacy.

To defend against malware, individuals and organizations employ antivirus software, firewalls, and other security measures. Regular software updates are crucial, as they often include patches to fix vulnerabilities that could be exploited by malware. Additionally, user education on

recognizing and avoiding suspicious online activities plays a crucial role in preventing malware infections.

In the ever-evolving landscape of cybersecurity, the battle against malware is ongoing. As technology advances, so do the methods employed by those with malicious intent. Vigilance, proactive security measures, and a comprehensive understanding of potential threats are key components in the ongoing effort to combat malware and protect digital environments.

1.3.2.1 Types of Malware

- **Viruses**: These are among the oldest forms of malware. Viruses attach themselves to legitimate programs or files and replicate when those programs run. They often spread through infected email attachments or malicious downloads. Once activated, viruses can corrupt or destroy files and may even disable antivirus software.
- **Worms:** Worms are standalone programs that replicate and spread independently. They do not need a host file to attach to, and they often exploit vulnerabilities in network protocols to move from one computer to another. Worms can quickly spread across interconnected systems, causing widespread damage.
- **Trojans:** Named after the ancient Greek story of the wooden horse carrying enemy soldiers, Trojans disguise themselves as legitimate software but carry malicious payloads. Unlike viruses and worms, Trojans do not replicate on their own. Instead, they rely on social engineering to trick users into installing them, giving attackers unauthorized access to the infected system.
- **Ransomware:** Ransomware encrypts a user's files, making them inaccessible until a ransom is paid. This type of malware has become increasingly prevalent and is often spread through phishing emails or malicious websites. Cybercriminals demand payment, usually in cryptocurrency, for the decryption key.
- **Spyware**: Spyware is designed to monitor and collect user activities without their knowledge. This includes keystrokes, browsing habits, and personal information. The gathered data is often sent to a remote server and can be used for identity theft, espionage, or other malicious purposes.
- **Adware:** While not as malicious as other types, adware is unwanted software that displays excessive and intrusive advertisements. It often comes bundled with free

software and can slow down systems or change browser settings. Adware is primarily a nuisance, but it can compromise user privacy.

- **Botnets:** A botnet is a network of infected computers, known as bots, controlled by a central server. Cybercriminals use botnets to carry out coordinated attacks, such as Distributed Denial of Service (DDoS) attacks, or to send spam emails. Infected computers become part of the botnet without the user's knowledge.
- **Rootkits:** Rootkits are a type of malware that hides its presence or the presence of other malicious software. They often manipulate operating system functions to avoid detection by security software. Rootkits can provide unauthorized access to a system, allowing attackers to control it stealthily.

1.3.3 Virus Definitions

Virus definitions serve as the backbone of antivirus software, acting as a comprehensive guide to identifying and combating malicious software. In essence, they are a digital encyclopedia that catalogues the characteristics and behaviours of known viruses, trojans, worms, and other malicious codes. Think of it as a constantly evolving library that your antivirus program consults to recognize and neutralize potential threats.

Each entry in this digital library contains unique signatures or patterns associated with specific types of malware. These signatures act as fingerprints, allowing the antivirus software to quickly identify and isolate malicious files or activities on your computer. Without up-to-date virus definitions, your antivirus program would essentially be working with an outdated library, unable to recognize the latest threats. Updating virus definitions is imperative due to the ever-evolving nature of malware. Cybercriminals continually develop new and sophisticated techniques to compromise systems and evade detection. Without regular updates, your antivirus software might not be equipped to recognize these novel threats, leaving your system vulnerable to potential attacks.

Consider it a proactive measure – updating virus definitions is akin to receiving the latest immunization against digital infections. By staying up-to-date with the newest information about malware, your antivirus software enhances its ability to detect, quarantine, and eliminate threats before they can cause harm to your computer or compromise your data.

In summary, virus definitions are the vital intelligence that empowers your antivirus software to safeguard your digital environment. Regular updates are essential to ensure that your system remains resilient against the dynamic landscape of cyber threats, providing you with a robust defence mechanism to preserve the integrity and security of your digital space.

1.3.4 Antivirus and its use

One day, while discussing computer security with her trusted IT administrator, Geeta pondered aloud, "Isn't there a way to keep our devices safe from the dangers lurking in the digital world?"

Moved by Geeta's concern, the IT administrator shared a timeless piece of wisdom: "Precaution is better than cure." Inspired by this adage, Geeta resolved to embark on a quest to fortify her digital fortress against external threats.

Geeta was determined to find the most effective means of protection. Consulting with experts and delving deep into the realm of cybersecurity, she learned of a powerful guardian known as antivirus software. Intrigued by its potential, Geeta wasted no time in acquiring this powerful tool.

With the the antivirus software set up on her devices, Geeta felt a sense of reassurance. With a vigilant watch over her digital domain, she knew that her valuable data and cherished devices were now shielded from the nefarious forces of the outside world.

Thus, armed with the wisdom of precaution and the strength of modern technology, Geeta continued her journey through the digital landscape, confident in her ability to navigate safely through its many perils.

Antivirus software is a crucial tool in cybersecurity, designed to detect, prevent, and remove malicious software, commonly known as malware, from computer systems. Its primary purpose is to safeguard computers and networks against various types of threats, including viruses, worms, Trojans, ransomware, and more.

Antivirus programs work by employing a combination of signature-based detection and behavioural analysis. Signature-based detection involves comparing the characteristics of files or programs against a database of known malware signatures. If a match is found, the antivirus software takes appropriate action to quarantine or delete the malicious file.

Behavioural analysis, on the other hand, observes the behaviour of programs in real time. If a program exhibits suspicious or malicious activities that do not match a known signature, the antivirus software may flag it as a potential threat.

Key uses of antivirus software include:

- **Real-time Protection:** Antivirus programs provide real-time protection by continuously monitoring system activities and incoming files. They automatically scan files and programs for potential threats, preventing malware from executing or spreading.
- **Regular Scans**: Antivirus software allows users to schedule regular system scans. These scans help identify and eliminate hidden or dormant threats that may not be immediately apparent during real-time monitoring.
- **Email and Web Protection:** Many antivirus solutions include features to scan email attachments and web content for malicious elements. This helps prevent users from inadvertently downloading or opening infected files.
- **Quarantine and Removal**: When a potential threat is detected, antivirus software often quarantines the affected files, isolating them from the rest of the system to prevent further damage. Users can then review and decide whether to delete or restore the quarantined items.
- **Automatic Updates:** Antivirus programs regularly update their databases of known malware signatures to stay ahead of new and emerging threats. Automatic updates ensure that the software is equipped to recognize and defend against the latest forms of malware.
- **Firewall Integration:** Some antivirus solutions include firewall capabilities to provide an additional layer of defence against unauthorized access and network-based threats.

In today's digital landscape, where cyber threats continue to evolve, using up-to-date antivirus software is a fundamental aspect of maintaining a secure computing environment. It serves as a crucial line of defence, protecting individuals and organizations from the ever-growing array of malicious activities perpetrated by cybercriminals.

1.3.3.1 Commonly used Antivirus for computers and mobile

Several antivirus programs are widely used for both computers and mobile devices to protect against malware and other cybersecurity threats. Here are some commonly used antivirus solutions:

- **For Computers**
    - **Norton Antivirus**: Known for its robust protection, Norton offers features such as real-time threat detection, firewall, and identity protection.

- **McAfee:** McAfee provides comprehensive antivirus and internet security solutions, including features like ransomware protection and a firewall.
- **Bitdefender:** Renowned for its high detection rates, Bitdefender offers a range of security products for various platforms, emphasizing minimal system impact.
- **Kaspersky:** Kaspersky is recognized for its advanced threat detection capabilities and includes features like a firewall, VPN, and parental controls.
- **Avast:** Avast offers a free antivirus solution alongside premium versions, with features such as real-time protection, Wi-Fi security scanning, and a password manager.

- **For Mobile Devices**
  - **Avast Mobile Security**: Avast extends its security offerings to mobile devices, providing features like antivirus scanning, Wi-Fi security checks, and anti-theft tools.
  - **Bitdefender Mobile Security:** Tailored for mobile platforms, Bitdefender Mobile Security includes malware detection, anti-theft features, and web security.
  - **McAfee Mobile Security**: Offering a range of protective features, including antivirus scanning, app privacy checks, and a secure media vault, McAfee is a popular choice for mobile security.
  - **Kaspersky Mobile Antivirus:** Kaspersky's mobile solution provides antivirus protection, anti-theft features, and web filtering for safer browsing on mobile devices.
  - **Sophos Mobile Security:** Sophos offers a free mobile security app with features like antivirus scanning, app privacy advisor, and secure QR code scanning.

It's essential to note that the effectiveness of antivirus software can vary based on individual needs, system requirements, and the specific features offered by each solution. Regular updates and staying informed about the latest cybersecurity practices contribute significantly to maintaining a secure digital environment.

1.3.5 Phishing emails

Abhay, Geeta's colleague, was smart with computers. But one day, he got tricked by a sneaky email. It seemed like a normal email, but it was a trick! The email promised him something exciting, so he clicked on a link inside.That was a big mistake. The link led to bad software that

messed up his computer. Suddenly, his computer was not safe anymore. It was like a secret attack from bad guys.When Abhay realized what happened, he told Geeta. She helped him fix the problem. Together, they worked hard to stop the bad software and make Abhay's computer safe again.

Abhay learned a lesson that day: not everything on the internet is safe. But he also learned that it's important to ask for help when things go wrong. With Geeta's help, he realised he had to be more careful in future.

Phishing emails are fraudulent messages designed to deceive individuals into revealing sensitive information, such as passwords or financial details. To recognize them, let us understand these key points**Phishing emails can attempt to trick recipients by:**

- **Impersonation**: Posing as a trustworthy entity, like a bank or a popular online service, to trick users into providing sensitive information.
- **Urgency or Fear Tactics**: Creating a sense of urgency or fear, pushing recipients to act quickly without thorough consideration.
- **Fake Websites:** Providing links to fake websites that resemble legitimate ones, aiming to capture login credentials or personal information.
- **Spoofed Email Addresses**: Faking the sender's address to appear as if the email is from a reputable source.
- **Malicious Attachments**: Including harmful attachments that, when opened, may install malware or compromise the recipient's system.
- **Social Engineering:** Exploiting psychological tactics to manipulate individuals into divulging confidential information willingly.

- Here are some steps to check if an email is a phishing attempt:
  - **Check the sender's email address:** Look closely at the sender's email address. Phishing emails often use slightly misspelled or fake email addresses that may resemble legitimate ones.
  - **Inspect the email content:** Read the email carefully. Phishing emails may contain spelling or grammatical errors, unusual formatting, or generic greetings like "Dear Customer" instead of your name.

- **Hover over links**: Before clicking on any links in the email, hover your mouse over them to see the actual URL. Phishing emails often include links that lead to fake websites that steal your personal information.
- **Check for urgent or threatening language:** Phishing emails often use urgency or threats to prompt you to take immediate action, such as claiming your account will be suspended unless you provide information.
- **Verify requests for personal information:** Be cautious if the email asks you to provide personal or sensitive information, such as passwords, Social Security numbers, or financial details. Legitimate organizations typically don't request this information via email.
- **Pay attention to logos and branding:** Phishing emails may include logos and branding to make them appear legitimate. However, these elements may be distorted or low-quality compared to genuine communications from the company.
- **Verify with the company:** If you are unsure about the legitimacy of an email, contact the company directly using a trusted phone number or website (not the contact information provided in the email) to verify the request.
- **Use email security features:** Enable spam filters and email security features provided by your email provider to help detect and filter out phishing attempts.

Remember to stay vigilant and trust your instincts when assessing the authenticity of emails.

1.3.6 Password

Passwords serve as the first line of defence against unauthorized access. Therefore, it is imperative to establish guidelines for creating strong passwords. Here are some guidelines discussed in detail.

- **Password Length:** The password length is generally 8 to 12 characters. It is recommended to have a longer password which is difficult to crack even thoughit is difficult to remember. An example of short and long passwords is given below:

  Short Password: "P@ss1"

  Long Password: "MyFav0riteF00dIsPizzaAndSushi!"
- **Password Complexity:** A strong password includes a combination of uppercase and lowercase letters, numbers, and special characters(!@#$%^&*, etc.). This makes it more difficult to crack. An example of weak and strong passwords is given below:

Weak Password: "password123"

Strong Password: "P@ssw0rd!23"

- **Avoidance of Common Passwords:** Avoid easily guessable words, phrases, or patterns like “password123”, “qwerty”, “123456789”, etc. Refrain from using passwords that include personal information such as your name, birthdate, or common words like nickname. Establish a policy that prohibits the use of these weak passwords to minimize the likelihood of unauthorized access.

  Some examples of passwords involving personal information that should be avoided.

  Sunita1992, Fluffy2021, SRMCollege1993, Mary1983 etc.

  A list of weak and strong passwords is given below:

Table 1: Weak Passwords and Strong Passwords

Weak Password	Strong Password
● Password123 ● Login ● admin	● P@ssw0rd!1234 ● Str0ngP@$$w0rd! ● AvaTar@1357#

Moreover, you should have different passwords for your accounts. Because if any one password is compromised, others are safe.

- **Multi-Factor Authentication (MFA):** Implement a multi-factor authentication system to augment password security. MFA requires users to provide additional verification, such as a one-time code sent to their mobile device, alongside their password. This adds an extra layer of protection, making it more challenging for attackers to gain unauthorized access.
- **Regular Password Updates:** To mitigate the risk of compromised passwords, enforce a policy that mandates regular password changes. This practice reduces the window of opportunity for potential attackers and ensures that users are regularly updating their credentials.
- **Secure Storage Practices:** Passwords must be stored securely to prevent unauthorized access in case of a data breach. Utilize robust encryption algorithms to protect stored

passwords, and avoid storing them in plaintext. Implement secure storage solutions that comply with industry standards and regulations.

- **User Education and Awareness:** Regularly conduct awareness programs to educate users about the importance of password security. Guide users on recognizing phishing attempts and emphasize the need to keep passwords confidential. Users should be aware of the potential risks associated with weak passwords and encouraged to report any suspicious activities promptly.
- **Restricted Access:** Limit access to sensitive systems and information only to personnel who require it for their roles. Implement a principle of least privilege, ensuring that users have the minimum level of access necessary to perform their job functions. This reduces the potential impact of compromised credentials.
- **Password Recovery Process:** Establish a secure and user-friendly password recovery process to assist users in regaining access to their accounts. This process should involve multistep verification to verify the identity of the user seeking password recovery, and preventing unauthorized access.
- **Audit Trails and Monitoring:** Maintain comprehensive audit logs that capture user authentication and access activities. Regularly monitor these logs to detect any unusual patterns or suspicious activities related to passwords. Implement alerts for potential security incidents, and conduct thorough investigations when necessary.
- **Periodic Reviews and Updates:** Security standards and threats evolve over-time. Conduct periodic reviews of password policies and update them based on emerging best practices and industry standards. Regularly assess the effectiveness of existing measures and make adjustments as needed to address new challenges.

In conclusion, a robust SOP for dealing with passwords is a fundamental aspect of any organization's cybersecurity strategy. By implementing these practices, organizations can significantly enhance their password security measures, reducing the risk of unauthorized access and potential security breaches. Regular updates and continuous education ensure that the workforce remains vigilant and adaptive in the ever-evolving landscape of cybersecurity threats.

Chapter 2: Psychological Aspect of Cyber Safety and Security

Objectives:

At the end of the session, learners will be able to:

- understand the impact of use of digital devices on mental wellbeing.
- recognise the mental health challenges associated with using digital devices and online platforms.
- identify ways to safeguard mental well-being while using digital devices and online platforms.
- identify red flag signs of mental distress while using digital devices and online platforms.
- learn self-care practices to protect mental well-being.
- identify experts to seek professional help to deal with mental health challenges associated with the use of digital devices and online platforms.

Outline:

- Mental well being in digital space
- Challenges to mental well being in digital spaces
- Safeguarding mental health
- Red flags sign of distress
- Seeking professional help

2.1 Introduction

Digital spaces have become an integral part of our lives. They offer a plethora of opportunities to improve our mental well-being. These spaces serve as sources of information, support, and connection, fostering a feeling of belonging and community. Online platforms provide a means for self-expression, enabling the sharing of positive experiences and resources, creating a virtual environment that uplifts, empowers, and inspires. While recognizing the benefits of digital spaces, it's crucial to tread carefully as we immerse ourselves. These spaces may present challenges to our mental health and overall well-being.

2.2 Mental well-being in digital space

Shruti recently received a smartphone on her birthday. She was very excited to use it. The shiny and sleek device opened up a new world of opportunities for her. It allowed her to connect with her friends at any hour of the day, explore new applications and look for information on the internet. The device became her companion in everything she did, shaping her experiences in positive and negative ways. On one hand, connecting with her friends on social media made her feel supported and cared for, but seeing others' perfect-looking lives made her feel a bit sad about her own.

She discovered new applications for relaxing and unwinding, and platforms where students talked about mental health and the importance of seeking mental health support. It helped her express herself better, deal with stress, and made her understand that she was not alone in the way she felt.. However, she felt pressured to constantly check her phone, respond to messages quickly. At times, this affected her sleep as well. She found it difficult to keep her phone away from herself. This also led to her feeling constantly tired, recurrent headaches and burning sensation in the eyes. She was worried her parents might scold her for not using her smartphone responsibly and hence, decided not to tell them about it. Deep down, she realized that she needed help. That is when she decided to reach out to her college counselor. She sat with her, discussed her problems, was able to strike a balance, limit usage, and use the smartphone in a way that made her feel good, while taking breaks whenever needed.

2.3 Challenges to mental well-being in digital spaces

Keeping up with the virtual world in the context of a hyper-connected world can be stressful. Overcoming **Fear of missing out (FOMO)** is a critical component of ensuring mental wellbeing while navigating digital spaces. Most of our social interactions occur online via messaging and social media applications. Individuals may often feel the constant need to check their notifications, messages and social media feeds to remain updated with social activities, events and experiences. They may find it **difficult to disconnect**, leading to **information overload** and **heightened stress levels**. There is a tendency for adolescents and youngsters to **prioritize digital interactions** over face-to-face communications. They may choose to capture and share their experiences rather than immersing themselves in pleasurable moments and being present in the here and now.

In addition, social platforms serve as a source of fulfilment of the need for social belonging and validation. The likes, comments, and shares can often become a measure of self-worth, leading to a **constant need for external validation.** It also creates an unhealthy **culture of comparison**, where individuals may never "feel good enough" when it comes to their lifestyles, appearance, relationships and achievements. These negative comparisons promote feelings of **dissatisfaction, jealousy, frustration** and may prove to be detrimental to overall mental well-being.

Social media and online platforms can negatively impact an individual's views about themselves and their bodies. Social media may contribute to creation of **unrealistic beauty standards**, leading to **dissatisfaction with oneself** and **low self-esteem**, and even psychological disorders such as depression, eating disorders, etc.

2.3.1 Digital addiction

It refers to a behavioral disorder characterized by an excessive and compulsive use of digital devices and online activities, to the extent that it interferes with an individual's daily life, work, relationships and overall well-being. It may be referred to as an umbrella term that subsumes issues such as problematic use of the internet, online gaming, smartphone, social media, online shopping, online pornography. Individuals often use their digital devices and online platforms as a way to escape from real life problems or distressing emotions.

These addictive behaviors are often associated with a sense of loss of control, excessive use, preoccupation with digital devices. This often leads to neglect of other responsibilities and interests, school work and household chores. Individuals may also find it difficult to disconnect. They may feel restless, anxious, or agitated when separated from their digital devices and feel pressured to check notifications and messages. They may experience a general loss of interest in activities such as hobbies, sports, etc. that were previously pleasurable. Eventually, they develop tolerance, which means that they need to use digital devices and online platforms for longer periods or engage in riskier online activities to achieve the same level of pleasure.

Digital addictions can have a negative impact on interpersonal relationships, which is an important determinant of mental health.

Individuals may also spend excessive money on new digital devices, purchases on online platforms, subscriptions, leading to negative financial consequences.

2.3.2 Cyber harassment

This refers to the use of online mediums and platforms such as social media, messaging and gaming platforms, etc. to bully, stalk, and/or groom individuals. It may include:

- **Cyber stalking:** Use of social media or other online resources to track an individual's location and monitor their activities in the digital space and/or real world. The aim is to induce fear and invade the privacy of the individual in question (victim).
- **Cyber bullying:** Creation and sharing of offensive messages, comments or content aimed at shaming, spreading rumors or excluding victims from online groups or activities. It may also include engaging in fights or arguments online with the aim of spreading hatred and provoking others.
- **Cyber grooming:** Process in which an individual builds a friendly relationship, often an emotional connection, with a child over the internet. The intention is to exploit the child for sexual purposes. Once the child trusts the groomer, they may be exploited to provide sensitive information, engage in sexual conversations, or explicit pictures or videos.
- **Catfishing:** It includes impersonating someone and sending messages to others or creating fake accounts.

The behavior is repetitive and is aimed to threaten, scare, shame, exploit and silence their targets. It has been associated with a wide range of negative impacts on an individual's mental health.

- **Stress and anxiety:** Constant exposure to online harassment, such as negative comments, trolls or messages can lead to heightened levels of stress and anxiety. It may cause uneasiness and hyper-awareness.
- **Depression:** Feelings of sadness, hopelessness over a long period of time.
- **Isolation:** Experiencing cyber harassment may lead to withdrawal of individuals from online and offline social activities, leading to a sense of loneliness or social isolation. Fear of judgment or further harassment can make it even more challenging to engage with others.
- **Low self-esteem:** Negative comments or views can significantly reduce an individual's self-esteem and confidence. It may also lead to feelings of self-doubt, helplessness and inadequacy.

- **Sleep disturbance:** Cyber harassment may disrupt sleep patterns. Individuals may find it difficult to fall asleep; or have poor disrupted sleep, or even have nightmares related to their online experiences.

Other potential consequences may include an inability to concentrate, perform basic tasks and other forms of physical symptoms such as headaches, stomachaches, or other ailments.

2.4 Safeguarding mental well-being in digital spaces

2.4.1 Self awareness and monitoring:

The first step to protecting one's mental health in digital spaces is to be aware of how much time is being spent on digital devices and online platforms, what is the purpose of use and whether the use is productive. At the same time, it is important to keep a check on the emotions that one feels while going through the content online or while using digital devices. Recognizing these emotions such as joy, excitement, jealousy, frustration, anger or sometimes even stress may help to filter out the content that one might want to consume. Monitoring the use of digital devices and the content consumed can play a critical role in ensuring overall well-being. This can be achieved in multiple ways.

- **Device usage tracking**. Many smartphones have in-built features such as Digital Well-being for monitoring screen time and usage patterns. There are some third party apps such as Digital Wellbeing (Google play store), Attentive- Digital Wellbeing (App store for iPhone and Apple Watch) which provide detailed insights into usage patterns and can be effective tools for monitoring device usage.
- **Insights from social media applications.** Many social media applications provide insights into usage patterns, number of screen unlocks, number of notifications, time spent on application, etc.
- **Web browser history.** Checking the web browsing history can be yet another effective tool to monitor usage. It provides users with a detailed list of websites accessed, which can help analyze the nature and type of content consumed by the individual.
- **Set Boundaries.** After monitoring device usage and online content consumption patterns, it is important to set boundaries to ensure limited and productive use. Setting these boundaries is crucial for building and maintaining a healthy relationship with technology. The goal is to strike a balance, so we use digital spaces for our benefit and betterment, and not spend too much time on devices. It is critical to prevent digital

addictions and promote mindful habits that lead to positive digital behaviours. This can be achieved by means of the following techniques:

- **App timers.** Most mobile phones have in-built settings that allow users to set specific time limits for usage of individual apps. Users receive notifications or experience restricted access once the allocated time limit is reached. It helps monitor and control app usage effectively.
- **Digital breaks.** Take regular breaks from digital devices. Engage in alternate activities such as reading, listening to music, reading, painting or engage in non-screen related hobbies during these breaks. Setting alarms or timers on devices can prove to be very useful to keep track of these breaks. They act as cues that help individuals become more mindful of the time spent on a particular task.
- **Designating device free zones.** Yet another way to limit device usage is to designate certain areas such as dining spaces, bedrooms or toilets as device free zones. This helps in creating boundaries and prevents excessive use.

It is important to keep track of these limits or boundaries, monitor digital habits, and make appropriate adjustments as and when needed to best suit the needs of the individual.

2.4.2 Mindful Consumption:

Use of digital spaces, whether by scrolling through social media accounts, watching videos or movies, or participating in online communication, can make one go through plenty of emotions. Therefore, it is important to pay full attention to what is happening in the present. This is often called the superpower of mindfulness. It helps an individual to not only be aware of the content being consumed but also their emotional response to it, which in turn creates positive online experiences and promotes mental wellbeing in digital spaces. Some ways in which one can cultivate mindful digital habits are:

- **Set intentions before use.** Before engaging with digital content, set clear intentions for purpose of use, nature of content and allocate a reasonable time for the activity. This prevents mindless scrolling and wasting time.
- **Be selective with Social Media.** Use of digital spaces, especially social media, can evoke various feelings from joy and excitement to frustration or even sadness. Ask yourself, “how do you feel?”. If something induces feelings of sadness or discomfort, it is

important to distance oneself. Unfriend, unfollow or mute accounts that contribute to negative feelings, and choose to be around positive and uplifting content.

- **Identify triggers of excessive use of digital spaces.** It is important to recognize that individuals frequently resort to digital spaces as a means of escaping real-life challenges or stressors. This escape serves as a temporary comfort, and as a result, individuals often engage with digital spaces excessively, in an attempt to avoid dealing with their problems. Triggers, which are stimuli that prompt us to spend more time on digital devices and online platforms than necessary, play a significant role in this behaviour. These triggers can range from feelings of boredom to conflicts with friends or family. They make people want to spend a lot of time using digital spaces. By acknowledging and understanding these triggers, individuals can gain valuable insights into the factors influencing their excessive use of digital spaces, paving the way for the development of mindful habits and more positive ways of coping.

2.4.3 Develop digital literacy and learn safe digital practices

Learn about online safety, privacy settings, and how to manage your online presence. Do not share private information such as personal photographs, current location, home address, phone numbers, PAN number, location, passwords; names, locations, contact details, address of family members and friends; credit and debit card numbers, CVV on credit cards, one time passwords, etc. on online platforms. In case of cyber harassment, inform elders or appropriate officials so that right actions can be taken. Being safe and feeling protected while using digital devices can promote a sense of mental wellbeing.

In the eventuality that individuals sense a potentially serious issue, like addiction to gaming platforms or social media, it is advisable to seek information from reliable sources such as the e-Health Intervention for Gaming Disorder at the Behavioural Addictions Clinic (BAC) All India Institute of Medical Sciences, New Delhi. Further relevant content on basics of management of behavioural addictions involving use of the internet has been included in the additional readings for reference.

2.4.4 Prioritize Real-world Connections

Nowadays, in social gatherings or family events, even if individuals are surrounded by loved ones, they prefer to remain engrossed in their digital devices. This becomes especially noticeable when someone feels a bit out of place or anticipates conversations that may feel awkward.

Digital spaces serve as a convenient means to avoid direct face to face interactions. Even when with friends, it becomes more important to capture memories and post them on social media rather than enjoying the moment. This is common behaviour and reflects a tendency to prioritize the digital world over real world interactions, often leading to loss of a sense of connectedness from friends and families in everyday life, which is critical to ensure mental well-being. Consciously prioritizing real life interactions, even in situations that one finds difficult or awkward, is a key step to cultivating a healthy balance between the digital and real world, and ensuring social and mental well-being. This can be achieved simply by keeping one's phone aside when in the company of friends and family!

2.4.5 Practice Self-Care

Include self-care activities into your routine. These could include exercise, meditation, or relaxation techniques. These practices can help manage stress associated with use of digital spaces and improve overall mental well-being.

- **Physical activity:** The nature of extended screen time use and engagement with digital spaces can negatively impact physical activity. Physical activity is known to release "feel-good" hormones or endorphins that improve the mood, promote happiness and well-being. Physical exercises can also act as a positive outlet for stress and anxiety. Indulging in physical activities during digital breaks can prove to be beneficial as it is not only an excellent alternative for use of digital devices but also provides an opportunity to build social connections in real life.
- **Breathing exercises and pranayama:** Focusing on breath, taking slow and deep inhalations can bring calmness and stability. Pranayam involves regulating breath while practising different postures (asanas) and meditation (dhyana). Here are some common pranayamas that can be practised regularly.
    - ***Anulom-Vilom Pranayama:*** Bend the index and middle finger of your right hand inward. Use your ring finger and thumb to block your nostrils. Inhale to four counts and exhale to 8 counts. Block your right nostril with your right thumb and inhale. Now release your right nostril and block the left nostril with your ring finger. Exhale. Now inhale on your right. And exhale on your left.
    - ***Ujjayi Pranayama:*** Imagine you have a glass in front of you and you want to fog it up with your breath. You have to do the same thing with your mouth closed. It

will sound like soft snoring sounds and you will feel a small constriction in your throat.

- ***Brahmari Pranayama:*** Cover your ears with your index finger. Inhale through your nose and exhale through your mouth making a humming sound.

- **Grounding techniques:** Grounding techniques help to reduce intensity of emotions and to view problems better by bringing about a sense of calm and peace. It uses the five senses, namely, sight, sound, smell, taste and touch to help unhook and unwind. Some ways to ground oneself are:
  - "Take a few deep breaths. Identify five things you can see, four things you can touch, three things you can hear, two things you can smell or like to smell and one thing you can taste.".
  - "Clap your hands and rub them. Feel the sensations. Feel the heat of your palms rubbing together."
  - "Give yourself a tight hug. Feel the warmth. Acknowledge the sensations and feeling of your arms being wrapped around you."

These activities help individuals come to the here and now, feel more connected to the present moment. They are particularly helpful for individuals who may be experiencing some kind of stress, or anxiety.

2.5 (Red flag signs of distress

While using digital spaces, individuals often face challenges. They deal with most of the problems alone. However, this journey is not always smooth and at times individuals may face distress that they might not be able to deal with on their own. That is when students can consider seeking help from mental health professionals. These could include:

- Spending excessive time on digital devices and online platforms and being unable to stop.
- Feeling sad, stressed or tired when using digital devices over a long period of time.
- Feeling anger, restlessness, irritation when away from digital devices and online platforms.
- Withdrawal from family, friends and social activities along with avoidance of school, work or social gatherings.
- Drop in academic performance
- Changes in appetite or sleep patterns

- Difficulty in concentrating on other tasks and chores
- Thoughts of self harm or suicide
- Distress due to any form of cyber harassment

It is important to note that these are not the only signs indicative of distress. Challenges related to digital spaces can interfere with daily life, relationships or overall well-being and can manifest in different ways in an individual's life. By staying attentive to any significant changes in how digital experiences impact different aspects of life, individuals can better understand when they need to seek support from mental health professionals.

It is also essential to emphasize that professional help is not only for times of distress but can also be sought to enhance overall well-being and find a healthy balance. Mental health professionals are valuable resources who facilitate personal growth, self-discovery and promote a positive mental state. They can help individuals build a protective shield in the form of tools and strategies to deal with challenges of the digital world or life in general.

Despite understanding the importance of seeking help from mental health professionals, the worry about how others will perceive, can deter an individual from seeking help in case of distress or crisis. It is important to note that it is a proactive and healthy choice; it signals strength and self awareness rather than a flaw. It is like going to a doctor when you are not feeling well.

It is also important to support and encourage those who reach out and seek support. This helps normalize help seeking for mental health concerns and breaks down barriers that prevent many from reaching out for the support that they need.

2.5.1 Seeking professional help

Seeking mental health is a brave and courageous step. Various professionals or experts in the field of mental health play distinct roles in providing support and offer different techniques or methods to help an individual. We will discuss the roles of different mental health professionals to help you navigate through the process of seeking mental health

- **Psychiatrists:** They are medical doctors who specialize in the field of mental health. They can diagnose mental health conditions such as depression, anxiety, and prescribe medications. They may also provide therapy.

- **Clinical psychologists:** They hold advanced degrees in psychology, and use different therapeutic methods to help individuals understand their thoughts and emotions. They are experts in human behaviour. They are trained to use strategies to help individuals deal with challenges such as relationship problems, parenting issues, stressful life situations and psychiatric illnesses. They are not medical doctors and do not prescribe medications.
- **Counsellors:** They may have diverse educational backgrounds, ranging from diplomas to masters in counselling. They provide guidance and support through talk therapy, offering a safe and confidential space for students to express their thoughts and emotions.

These experts will help you by providing education about safe online behaviours and practices. They will equip you with practices such as mindfulness, relaxation to manage stress and deal with problems in everyday life.

Chapter 3: Physical Aspect of Cyber Safety and Security

Objectives:

At the end of the session, learners will be able to:

- understand the impact of use of digital devices on various aspects of physical health, for example, sleep, eyes, ears and lifestyle.

- gain awareness of posture related issues associated with long term use of digital devices and online platforms.
- incorporate objective strategies to safeguard physical health while using digital spaces
- Use the right postures while using digital devices.
- practice yoga asanas and simple exercises to improve posture and prevent injury related to long term use of digital devices.

Outline:

- Impact of digital spaces on physical health
- Safeguarding physical health while using digital spaces.

3.1 Introduction

Imagine spending the whole day in a dimly lit room, attending online classes. Glued to the screen, munching on chips and sipping cold drinks during breaks. Shuffling on the bed for comfort when you feel tired. In the evening, joining online coaching classes and solving worksheets on tablets or laptops. When bored, finding comfort and entertainment in a webseries episode. Nights reserved for marathon video game sessions or catching up with friends by sharing relatable memes and reels. Does this sound familiar?

Digital spaces have become an integral part of our lives. The frequency and duration of our use of digital devices and our engagement with online platforms is increasing. The convenience of digital devices and technology provides an opportunity for swift transition between different activities such as attending online classes, to watching web series and engaging in online gaming with friends. Digital spaces impact various aspects of our lives, including our physical health. These include our sleep, eating habits, lifestyle choices, vision, hearing, and posture.

3.2 Impact of Digital spaces on physical health

3.2.1 Sleep

Use of digital spaces impacts sleep in multiple ways. It is influenced by various factors. First, exposure to blue lights emitted by the screens can interfere with the production of sleep hormone melatonin. This disrupts the sleep-wake cycle, also known as the circadian rhythm.

Second, the stimulating nature of content on online platforms can keep the brain active, interested, excited and curious, making it difficult to get a good night's sleep.

Third, digital devices enable instant access to information, news and social interactions. This may sometimes lead to stress or anxiety, which in turn negatively impacts sleep. Constant notifications from smartphones can disrupt sleep by causing an individual to wake up multiple times during the night by prompting them to check their devices.

Fourth, negative online experiences such as cyberbullying or online harassment can lead to fear, anxiety, stress, thereby affecting sleep quality. Fifth, individuals may intentionally stay up late, and use their devices for leisure and relaxation. This could include them engaging in online gaming or binge-watching digital content. This can lead to delayed bedtime and reduced duration of sleep.

Lastly, frequent use of digital devices in bed may lead to awkward and incorrect neck and spine positions, resulting in pain in the neck, shoulders and upper back, and affecting sleep quality. Therefore, in conclusion, extended exposure to digital devices may lead to difficulty in falling asleep, reduced sleep quantity and quality, increased likelihood of experiencing insomnia, disruption of circadian rhythm, poor sleep hygiene and daytime sleepiness.

3.2.2 Lifestyle

Digital spaces influence various aspects of daily life and shape how individuals interact, work and spend their leisure time. Digital spaces offer a wide variety of options for entertainment including gaming, social media, online communication, video content, movies and web series. It cater to diverse interests. However, this may lead to an inactive lifestyle; spending most of their time glued to the screen prioritizing use of digital devices and online platforms for leisure over engaging in real-world activities. This inactive lifestyle has been associated with health issues such as obesity, heart problems, muscular and skeletal disorders, etc.

Digital spaces have a significant impact on nutritional and food choices. The sheer convenience of ordering food from anywhere and at any hour of the day can contribute to unhealthy eating choices and patterns. In addition, advertisements on various platforms that promote consumption of unhealthy or “junk” food as “cool”, “fun” and “tasty” contribute to unhealthy dietary practices. Excessive sedentary time spent in the digital space, coupled with limited physical activity, further contributes to excessive weight gain.

3.2.3 Eyes

Extended exposure to screens can lead to various eye related issues referred to as digital eye strain or computer vision syndrome. Reduced blinking rate due to staring at the screen for long

periods of time can lead to dryness, irritation or burning sensation, strain, sensitivity to bright light and tired eyes. It can also lead to blurred vision and difficulty in focusing from one distance to another. Musculoskeletal symptoms such as headache, neck or shoulder pain and back pain may also be associated with computer vision syndrome.

3.2.4 Ears

Digital spaces can affect ears due to exposure to prolonged and loud audio through electronic devices, especially the use of headphones or earphones. Exposure to loud music or sounds can damage delicate structures in the inner ear, leading to impaired hearing ability, or a persistent ringing or buzzing sensation in the ears, which is referred to as tinnitus.

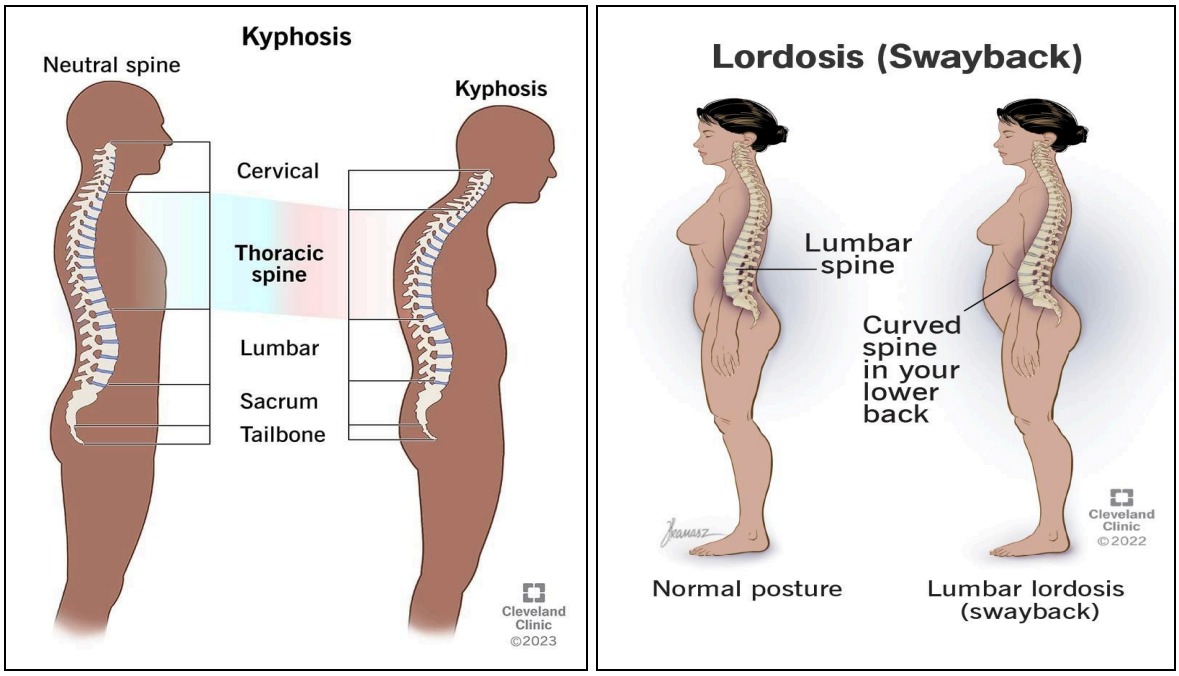
Regular use of headphones or earplugs at high volumes can lead to difficulty in hearing faint sounds in the environment. This can be dangerous as it affects awareness of what is happening around and compromises safety of individuals. In addition, use of in-ear audio plugs over a long period of time can create an optimal environment for growth of bacteria. This may even cause ear infections, resulting in pain and discomfort.

3.2.5 Postural issues

Use of digital devices and engagement with online platforms over a prolonged period of time can contribute to various postural issues. This is due to Repetitive Strain Injury (RSI) or forceful, awkward, and/or repetitive use of limbs. It causes damage to the muscles, tendons, and nerves. The severity of RSI cases varies widely. RSI can occur frequently due to extended use of digital space owing to repetitive movements.

3.2.6 Neck and shoulders

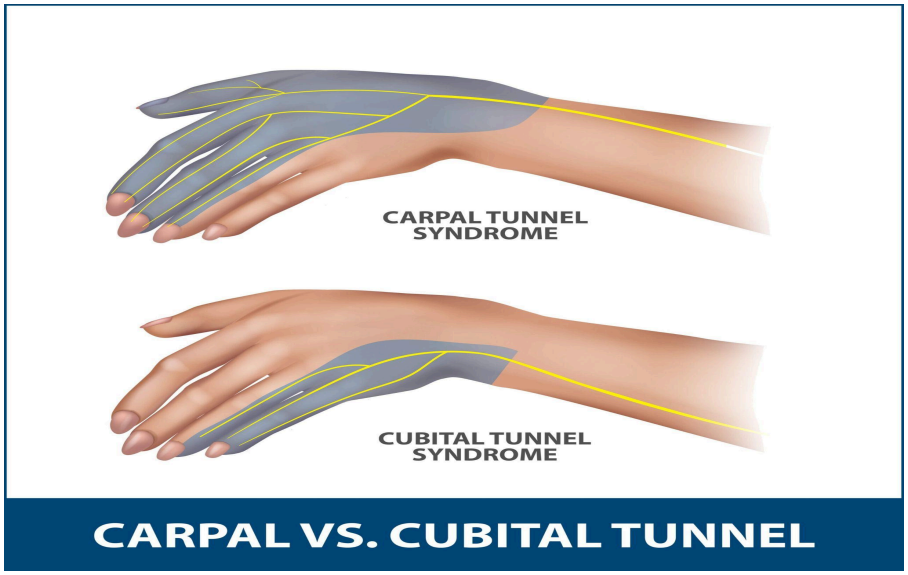
(Note- the images used in the file are all indicative. These may not be free for use. These need to be replaced with similar images that need to be created.)



Retrieved from: https://my.clevelandclinic.org/health/diseases/17671-kyphosis https://my.clevelandclinic.org/health/diseases/23908-lordosis

- **Text neck**. Hand held devices such as smartphones or laptops require the user to look down and slouch, i.e. keep a low head posture for a long period of time. This may cause headache, neck pain, shoulders and may also affect breathing.
- **Turtle neck**. Over-extension of the neck resulting in a posture similar to a turtle. It may lead to increased tension in shoulder and/or neck muscles, headaches, pain and discomfort in the neck, arms, upper back or shoulders.
- **Rounded shoulders.** Use of digital spaces over an extended period of time causes the shoulders to be positioned forward, and rounding of the upper back. Excessive rounding of the upper back associated with prolonged sitting and slouching is called Kyphosis. This may contribute to pain in the upper back and shoulders.
- **Mouse shoulders.** Pain, tension and stiffness in the shoulder and neck due to prolonged use of computer mouse.

3.2.7 Hands and wrists



Retrieved from: https://www.floridaortho.com/specialties/elbow-pain-treatment/cubital-tunnel-syndrome/

- **Cell phone elbow.** Bending the elbow for long periods of time when using digital devices can lead to pinching of nerves causing tingling sensations or numbness in the hand. This is also referred to as **cubital tunnel syndrome.**
- **Smartphone pinky**. Numbness, pain or tingling sensation in the little finger. This could be a symptom of cell phone elbow or result from compression of nerves due to supporting the smartphone with the little finger over a long period of time.
- **Texter's thumb.** Pain, cramping, weakness or numbness in the thumbs and wrist due to repetitive movement while texting or using smartphones.
- **Carpal tunnel syndrome.** Tingling sensation and numbness in thumb, index and middle finger.

3.2.8 Back

- **Lordosis:** Excessive inward curving of the lower back, often associated with sitting for extended periods with poor lumbar support. It may cause lower back pain and discomfort.

3.3 Safeguarding physical health while using digital spaces.

The use of smartphones, computers and other digital devices have transformed the way we work, connect to others and keep ourselves entertained. The constant interactions with screens and

prolonged use can pose significant challenges to the physical well-being of individuals. We shall now discuss some practical approaches to safeguard physical health while using digital spaces.

- **Ergonomics and use of digital spaces**: Ergonomics refers to the scientific study of people in their working environment. The goal is to understand the interactions between humans and other elements in the environment to improve performance and overall well being, and reduce discomfort and risk of injury due to work. Digital spaces have become an integral part of almost all aspects of our daily lives, such as studying, completing assignments, entertainment, interacting with people, etc. Using digital devices over an extended period of time may expose one to the risks of physical health issues associated with use of digital spaces such as reduced concentration, discomfort, fatigue, etc. Incorporating ergonomic practices by making small tweaks to one's postures, device placement and work environment can help develop healthy digital habits, promote mindful use of technology and overall well-being. It can improve the quality of interactions with digital spaces, thereby enhancing engagement, learning outcomes and productivity. Overall, it also promotes a positive relationship with technology. Some ways in which ergonomic practices can be incorporated are:

3.3.1 Postural awareness

It is important to pay attention to one's posture while using digital devices such as smartphones, laptops, computers, etc. and consciously maintain correct postures, especially when using digital spaces for an extended period of time.

While using desktop computers, sit upright and look straight ahead. Place the screen right in front. To do this, one may use a laptop stand or place some books under the monitor or laptop so that one can remain straight while using digital devices. Avoid bending the neck or trunk. Keep shoulders relaxed and in a neutral position. Keep the feet flat on the floor and thighs parallel to the floor. Elbow should be close to the sides. Avoid resting elbows on a hard surface or edge of the table. Wrists should be in a neutral or straight position. While typing, avoid keeping the wrist on the table or taking any support. This can result in bending of the wrists either up or down or side to side, which may cause discomfort or pain in the longer run. Take brief breaks while working.

While using handheld devices such as smartphones or tablets, one must sit or stand upright. They must not slouch or slump. Alternate fingers when using buttons and/ or touchscreens. Reduce typing or keystrokes, use speech recognition whenever possible. Use hands-free devices such as earplugs or headphones, to prevent holding devices for extended periods of time. Hold the device directly in front of the face when using it. Avoid excessive looking down when reading texts, emails or other information on the device. It is also important to take frequent breaks from using devices.

Check posture every 20 minutes. If it is incorrect, move around and adjust to ensure correct posture.

Additionally, including certain yoga asanas in the regular routine can be beneficial for improving posture and ensuring physical well-being while using digital devices.

- **Tadasana:** "Stand upright, with your feet together. Inhale as you raise your arms from the front to the top of your head. Intertwine your fingers such that your palms are facing outwards. As you lift your arms, lift your heels off the ground. Balance your body weight on your toes. Maintain this position for 20-30 seconds. Exhale as you bring your heels and your arms down."
- **Vrikshasana:** "Stand comfortably. Place your right foot on the left inner thigh such that you are standing on one leg. Keep your spine straight and bring your palms together on your head to form a namaskara pose. Maintain pose for 20-30 seconds. Repeat with the other leg."

- **Bhujangasana:** “Lie flat on your stomach. Keep your legs close together, palms near the shoulders and elbows close to the body. Breathe in as you raise your head, chest and abdomen off the ground. Keep your elbows bent and ensure that your lower body remains in contact with the mat. Feel the stretch in your spine. Exhale as you gently lower your upper body on the ground. Relax.”
- **Marjaryasana-Bitilasana:** “Place your palms and knees on the ground. Keep your wrists directly under your shoulders and your knees under your hips. Spread your fingers as wide as possible. Inhale as you round your spine towards the ceiling, Drop your head, bringing your chin to your chest. Engage your abdominal muscles to create a deep stretch in your back. This is the cat pose. Now Exhale as you lift your head, extend your neck and arch your lower back. Let your belly sink toward the floor. This is the cow pose. Move back to the neutral position, almost like a table top. Repeat this asana a few times.”
- **Setu Bandhasana:** “Lie on your back, bend your knees, and place your feet hip-width apart. Place your arms on your sides with the palms facing down. Press your feet on the ground and lift your hips toward the ceiling.”

3.3.2 Workspace organization

Position the monitor so that your neck is in a neutral and straight position. Ensure that there is no glare or reflections on the screen from windows or lights. Use a chair with adequate back support. Place input devices such as keyboard, mouse or other pointing devices in a manner so as to avoid excessive reaching. Customize your screen background, colour, font size, pointer size to ensure comfort and efficiency.

3.3.3 Taking breaks and movement

It is also important to take breaks when using devices for an extended period of time. Stand up, stretch or perform some simple exercises to reduce the long-term impact of prolonged device use. Include exercises that strengthen your neck, back, hands, legs, wrists, shoulders, feet and fingers. These exercises help to improve posture and flexibility, release tension and muscle pain.

3.3.4 Wrist and fingers

- Finger stretches: “Start with your elbows parallel to the ground and palms facing upwards. Spread out your fingers as much as you can. Slowly move your fingers as if you are clutching a small object such as a pillow or a sponge. Now relax and repeat the action five times. Repeat the same exercise with your palm facing downwards.”

- Finger fan: “Spread your fingers as wide as possible and then make a fist. Repeat the action 10-15 times.”
- Wrist Flexion: “Keep your elbow straight, bend your wrist towards the floor. Now use the opposite hand to pull the hand towards your body. Feel the stretch in your forearm and wrist.”
- Wrist Extension: “Keep your elbow straight, bend wrist up towards the ceiling. Use the opposite hand to pull the hand towards your body. Feel the stretch in the bottom of your forearm and wrist.”

3.3.5 Back

- Stretch Up: “Sit up straight and raise your hands. Intertwine your fingers and stretch to be as tall as possible. Hold for a few seconds and relax.”
- Backward Arch: “Stand straight. Place your hands on your hips to support your lower back. Look up at the ceiling while slowly leaning backward. Don’t force yourself beyond your personal range. Hold this stretch for 15- 30 seconds. Relax.”
- Shoulder Squeeze: “Raise your arms in front of your body. Keep your elbows slightly bent with your thumbs up. Pull elbows back, squeezing shoulder blades together. Hold for a few seconds and then release. Relax.”

3.3.6 Neck

- Neck Tilt: “Sit up straight. Gently tilt your neck to one side. Try to bring your ear towards your shoulder. Hold the position for 15-30 seconds. Keep your head in neutral position for a few seconds. Now gently tilt your next to the other side.”
- Head Rotation: “Slowly rotate your head to the right, as far as comfortable, then to the left. Repeat five to ten times.”
- Head Flexion: “Bring your chin down towards your neck. Hold this position for 10- 30 seconds as per your comfort. Release and relax.”
- Head and Neck Extension: “Tilt your head back so that you are looking up to the ceiling. Hold the position for 10- 30 seconds as per your comfort. Release and relax.”

3.3.7 Shoulder

- Shoulder Rotation: “ Extend your arms to the sides. Bring them to your shoulder’s height. Begin making small circular motions with your shoulders in the forward direction. Perform 10-15 rotations and then reverse the direction.”

- Crossover Arm Stretch: “Relax your shoulder. Extend your right arm straight in front of you at shoulder height. Keep your palm facing down, fingers together, and the elbow slightly bent. With your left hand, gently pull your right arm towards your chest using your left hand. You should feel a stretch across the back of your right shoulder and upper arm. Hold the stretch for 15-30 seconds. Focus on breathing deeply and relax into the stretch. Now repeat on the other side.”
- Shoulder Rolls: “Lift your shoulders up towards your ears. Roll your shoulder backwards in a circular motion. Continue this motion for 10-15 repetitions. Now roll your shoulders forward in a circular motion.”

3.3.8 Legs and feet

- Toe Curl: “Stretch your feet. Curl toes under. Then release. Repeat this exercise a few times.”
- Foot Rotation: “Keep your right leg on your left thigh. Circle your foot slowly from the ankle. Reverse the direction of the circles. Relax.”
- Hip Stretch: “Keep your right leg on your left thigh. Put your right hand on your right knee and left hand on your right ankle. Apply gentle pressure on your knee and move it up and down so that you feel a mild stretch on your right hip. After a few repetitions, relax and keep both feet on the ground. Repeat with your left leg.”

3.3.9 Protection of eyes

To prevent dryness and lubricate eyes, consciously blink regularly and use eye drops. Ensure adequate lighting in the room to reduce eye strain and glare. Adjust screen brightness based on convenience and use blue light filters, especially in the evening. Incorporate regular eye exercises such as:

- Eye rolls: “Roll your eyes clockwise. Count till five. Now roll your eyes counterclockwise.”
- Rub your palms together to generate some heat. Cup your palms and keep them lightly over your eyes without touching them for 30 seconds.
- Look away from your screens periodically. Take a break every 20 minutes, look at something 20 feet away for at least 20 seconds. This is called the 20-20-20 rule.

Schedule regular eye examinations to identify and proactively deal with vision problems.

3.3.10 Protection of ears

Limit use of headphones or earphones by taking regular listening breaks. Use hearing devices at moderate volumes. Regularly clean listening devices to prevent build-up of bacteria to reduce the risk of ear infections.

3.3.11 Sleep hygiene and safe practices

Understanding the impact of digital spaces on sleep allows individuals to adopt healthier digital habits and create a conducive environment for quality sleep. Establishing a digital curfew by specifying and limiting hours of use of digital devices, using blue light filters, and avoiding use of devices prior to bedtime can help reduce the negative effects of digital spaces on sleep.

3.3.12 Proper hydration and nutrition

Mindful habits such as taking breaks for adequate intake of water and other fluids such as fruit juices, and consuming a balanced diet is essential to sustain energy for efficiently using digital spaces. It helps improve and regulate brain and body functions. It boosts the immune system, plays a crucial role in managing stress, helps improve quality of sleep and overall well-being.

3.3.13 Schedule health check ups

Incorporating these practices into daily routine while using digital spaces will help improve physical health and overall well-being. However, we must always pay attention to the body's signals. If one experiences persistent discomfort, numbness or weakness that negatively affects daily activities and functioning, consult a medical professional.

Chapter 4: Socio-Ethical Aspect of Cyber Safety and Security

Objectives:

At the end of the session, learners will be able to:

- Understand ethical considerations related to technology usage.
- Define netiquette and its importance in online communication.
- Identify different types of netiquette: Email, social media, and gaming.
- Understand the concept of digital privacy and its significance.
- Develop critical thinking skills to evaluate online information.
- Define digital footprint and its impact on personal and professional life.
- Define plagiarism and recognize its ethical implications & its different forms.

Outline:

- Ethical Use of Technology
- Netiquette
- Privacy in the digital world
- Critical Thinking in the Digital Age
- Fact-checking of Information
- Digital Footprint
- Avoiding Plagiarism

4.1 Introduction

In today's digitally-driven world, understanding how to navigate the vast landscape of technology with integrity and responsibility is crucial. Through this module, we will explore various facets of digital citizenship, including the ethical use of technology, netiquette principles encompassing email, social media, and gaming etiquette, as well as the importance of privacy in the digital sphere. Additionally, we will delve into critical thinking skills tailored for the digital age, focusing on fact-checking information to discern truth from misinformation. Furthermore, we will examine the concept of digital footprint and its implications on personal and professional life, while also addressing ethical considerations surrounding plagiarism. By engaging with these topics, we will develop the knowledge and skills necessary to navigate the digital world thoughtfully and ethically, ensuring our digital interactions contribute positively to both ourselves and the broader online community. Welcome to the journey of becoming responsible digital citizens!

4.2 Ethical Use of Technology

Ethics are a necessary part of everyone's existence. The ethical principles that guide a person's conduct of activity, impact people's behavior and assist them in choosing the best decision. It governs an individual's decisions at every step of the process, even in the classroom. With increased use of digital technologies, there is growing concern about its ethical service. Teachers and parents must work together to educate youngsters to awaken their inner consciousness.

The majority of this generation's children grew up with technology. They know how to take advantage of everything. The biggest difficulty that these students will face while using technology in the classroom is that the border between school and personal life may get blurred. This must be kept in mind by the pupils at all times. They should use caution when using the email system and should only visit suitable websites. Putting someone down can never bring you to the top, but some people continue to do so through many activities (such as cyber bullying, cyber stalking etc).

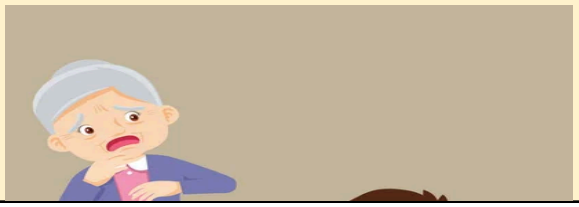
While social networking sites are a fantastic way to stay in touch with friends and family, they are also used as a platform for cyberbullying. Another concern with these sites and online forums is confidentiality; they collect a lot of user data.

It contains principles and recommendations for courteous and proper internet conversation. It is not a policy; it is managed by the internet community as a whole. It would still be crucial because internet communication is nonverbal.It is equally important for a person to manage their behavior when using technology in class and while utilizing online platforms and caring for the equipment.

Both students and instructors must be cautious about what they download. Downloading malware or viruses by accident might be disastrous. The school administration can employ antivirus software to safeguard the technology from such threats. Furthermore, they should never stop doing routine technological maintenance.

4.3 Netiquette

One day Mrs. Saran went to her friend's house and she saw one kid playing in the garden. She cheerfully greeted the kid but



suddenly the kid started misbehaving with Mrs Saran. She got upset and discussed the story with her friend. Her friend stated that the kid has been misbehaving strangely for the past few days. This type of behaviour is not justifiable. We can say that the child does not have etiquettes at all. Everyone should behave with others in an appropriate manner. In the same way when we use the internet and interact with others we have to behave in a decent way.
Photo credits: https://depositphotos.com/

Netiquette = N + etiquette where N is used for net and etiquette describes the rules of conduct for respectful and appropriate behavior. Sometimes, it is also referred to as Digital etiquette or Online etiquette. These are not defined rules but recommended rules of etiquette. In simple terms, this means being aware of and acting in a responsible, appropriate and ethical way while using digital technology. This also involves establishing your digital reputation and acting as a responsible member of the communities in which you engage, which might range from school groups to social networks to games. Following are the types of etiquettes:

Email Etiquette

- Always identify yourself and keep your messages brief and to the point.
- Include a concise subject line with all of your emails. This will allow the recipient to quickly scan their mailbox to see if the message is something they need to act on or "junk" email.
- Avoid sending insulting, abusive, or threatening remarks. Once a mail is sent, it can not be undone. The 'Undo' option in email is available for a maximum of thirty seconds after sending the mail.
- Remember that email is not necessarily private. Your messages can be forwarded to many people without your knowledge. Before sending a message, read it over, double-check the recipient(s) and make sure it would not become an embarrassment if it were forwarded to others not on your recipient list.
- Do not spam others. Spam is the practice of sending unsolicited email messages in bulk or overloading someone's mailbox or server with messages.

Social Media Etiquette

- While you are using Social Media, during chatting and messaging you should always remember that the person on the other side is just like you, speak to them in a manner that you want to be spoken to; or the way you would treat a person if you come face to face.
- Stranger Danger Online: You should always be mindful of whom you accept as friends online. It might seem a good idea to talk to strangers, but one needs to exercise caution in the virtual world. There have been many instances where people have been victims of fraud.
- It has become a trend to treat one's social media accounts as a personal diary. Children often put out their thoughts and feelings without thinking about the repercussions. It is not always a good idea to be vocal about all your thoughts and feelings online.
- Do not use your social media accounts to vent out your anger. While at the moment it might look like a good idea, you might regret it later. If you find it difficult to control and feel the urge to yell out, turn off your phone for a few hours.
- When you feel overly emotional, you might express your feelings through social media; rather opt to meet a trusted adult to express your feelings.

Gaming Netiquette

- Respect other fellows and game rules: Games are meant for your pleasure so you should not show your superiority over fellow players and you should follow the rules. Treat fellow gamers with respect, regardless of their skill level, age, gender, or background. Avoid using offensive language, bullying, or engaging in behavior that could make others feel uncomfortable. Be patient with less experienced players and offer constructive feedback instead of criticism.
- Respectful Communication: Use in-game chat or voice communication respectfully. Communicate clearly and politely with your teammates and opponents. Avoid spamming or flooding chat channels with unnecessary messages.
- Be a Team Player: Work together with your team towards common objectives. Support your teammates, offer help when needed, and avoid actions that could harm your team's chances of winning.
- Accept Defeat Gracefully and Celebrate Victories Humbly: Defeat and victory are two sides of a coin so you should not react aggressively in both situations.

4.4 Digital Privacy

Maya was a talented student who ran her own blog for the artwork. She was passionate about her work and loved connecting with other students and helping them create new artworks from all around the world through her website and social media platforms.

Maya took great pride in her craft. She understood the importance of privacy in the digital world and took every precaution to protect her and other students' personal information. She encrypted sensitive data and regularly updated her website's security features to prevent unauthorised access.

One day, Maya received an inquiry from another person named Alex, who was interested in working with her for a cartoon book. Alex seemed friendly and enthusiastic about collaborating with Maya, so she agreed to discuss the project further via email.

Maya and Alex exchanged messages for the craftwork. Alex started asking for more personal information with emotional chats. He wanted to know her full name, address, and phone number.. Maya felt uneasy about sharing such sensitive information with a stranger.

Maya discussed the issue with her teacher. The teacher made her aware about the importance of respecting boundaries and privacy online. He advised Maya to politely decline to provide the requested information and end the conversation with Alex.

She politely informed him that she wouldn't be able to proceed with the project and wished him the best of luck.

As Maya reflected on the encounter, she realized the importance of setting boundaries and protecting her privacy, even in the digital world. She understood that safeguarding personal information wasn't just about following security protocols—it was also about respecting her own boundaries and consulting her elders or trustworthy person when something didn't feel right.

Privacy entails recognizing the right to control personal information. It involves safeguarding sensitive details like name, address, and phone number from unauthorized access. Vital for security and identity protection, privacy awareness helps mitigate risks of online threats such as identity theft and cyberbullying. Children learn to discern which information is safe to share online, respecting boundaries and obtaining consent before disclosing personal details about others. They grasp the significance of digital footprints and adopt safe practices, like strong

passwords and cautious browsing. Ultimately, understanding privacy empowers children to navigate the online world responsibly, ensuring their safety and respecting others' privacy.

Points to be kept in mind:

- Never upload or post pictures of your friends without their consent.
- Never take screenshots or snapshots of your friend’s pictures, it might be your phone but the picture belongs to others.
- Don’t take inappropriate pictures or upload such pictures online. This rule applies to both your pictures and your friend’s pictures.

4.5 Critical Thinking in the Digital Age

The most important tool you have in the information age is the ability to think critically. It gives you the ability to confidently traverse the information sea, make wise decisions, and actively participate in conversations and debates. Remember that being a critical thinker involves more than just knowing things; it also involves thinking critically as you pursue your education and future endeavors. Accept the challenge of the information age and use critical thinking to navigate an information-rich environment.

Critical thinking is the art of thinking about thinking. It involves actively and objectively analysing information, concepts, situations, or problems to make reasoned judgments.

- **Recognizing Bias and Misinformation**: Bias can slant information in one direction, while misinformation presents false or inaccurate data.
- **Diverse Sources:** Seek information from a variety of sources to get a more balanced perspective.
- **Fact-Checking:** Verify information through fact-checking websites or trusted sources.
  Question Everything: Challenge your assumptions and question the motives of those presenting information.
- **Evaluating Sources:** Not all sources are created equal. When assessing the reliability of a source, analyze Authorship and credibility.
- **Analyzing Arguments:** Critical thinking involves the ability to analyze arguments and identify logical fallacies. Logical fallacies are errors in reasoning that can weaken an argument.

- **Developing Critical Thinking Habits:** Critical thinking is not a one-time event but a habit that can be cultivated. Here are some ways to practice and develop your critical thinking skills:
- **Read Widely:** Explore diverse viewpoints and read material that challenges your beliefs.
- **Engage in Discussions**: Participate in debates, discussions, and forums to practice thinking on your feet.
- **Ask Questions**: Don't be afraid to ask questions and seek clarification when something isn't clear.
- **Reflect:** Take time to ponder what you've learned and how it fits into your existing knowledge.
- **Fact-checking of Information:** Some tips to sorting out facts, evaluating resources and becoming more knowledgeable about the resources you use to find information.
    - ❖ Check Credentials: Verify the expertise and qualifications of the author or organization presenting the information to ensure accuracy and reliability.
    - ❖ Read the "About Us" section: Understand the background and mission of the source to determine potential biases or agendas.
    - ❖ Look for Bias: Assess the information for any signs of bias, whether political, commercial, or ideological, that may influence the content.
    - ❖ Check the Dates: Ensure the information is up-to-date and relevant by checking publication dates, especially for topics that evolve over time.
    - ❖ Check out the Source: Investigate the reputation and credibility of the source, such as established news outlets or peer-reviewed journals.
    - ❖ Examine URLs: Verify the domain and website structure for reputable sources, as unreliable or suspicious URLs can indicate potential misinformation.
    - ❖ Suspect the sensational: Be cautious of exaggerated or sensationalized claims and seek corroborating evidence from multiple reliable sources.
    - ❖ Judge Hard: Apply critical thinking and skepticism to evaluate the accuracy, consistency, and completeness of the information before accepting it as fact.

4.6 Digital footprint

A digital footprint is the recorded and traceable activities of a particular person on the internet or other devices. It is your data trail on the Internet and almost every action you take on the Internet, whether visiting a website, subscribing to a newsletter, or searching for a product, leaves a track of data. By following your data trails, anyone with access to a search engine or specialized technology, such as a skip tracing tool, can monitor your behavior, preferences, opinions, and much more.

Digital footprint examples include

- Search History
- Browsing history
- Text messages
- Creating online accounts
- Photos and videos uploaded online
- Using digital fitness trackers
- Content liked and posted on social media
- Subscribing to blogs or newsletters
- Comments or reviews left online
- Buying and selling online stocks
- E-commerce purchases and activity
- Signing up for apps (e.g., shopping, dating, and health apps)
- Photos where users are tagged

Examples of data that go toward digital footprints can also extend to deleted content. Just because it's gone from one place, or the original place, doesn't mean it's been completely erased from existence. Data gets copied and shared for a number of reasons, making even deleted content part of your digital footprint.

4.6.1 Types of digital footprints

There are two types of digital footprints**- passive and active digital footprints**, which differ by informed consent. The online data-sharing activities you do intentionally or with informed consent make up your active digital footprint. The definition of a passive digital footprint refers

to the data collected when your online activities are tracked without your informed consent or knowledge.

a. Active digital footprint

An active digital footprint is a content you generate and online activities you deliberately engage in. If you're an online over-sharer, you have a massive active digital footprint. If you keep online sharing to a minimum, you would mostly leave behind internet cookies and trails for ad tracking (passive), but you'll still have an active footprint to some degree.

Data deliberately or knowingly shared by users is the crux of the active digital footprint definition — examples include:

- Posting on social media or online forums
- Completing online forms
- Emailing
- Online Gaming

b. Passive digital footprint

A Passive digital footprint is all the information collected about you without your explicit knowledge or active involvement. This is considered passive because you are not aware that this information is being collected.

Some common sources where data is gathered stealthily include:

- Website usage details (IP address, how many times you visit a website, how you arrive at a website)
- Smart home devices
- Financial records

4.6.2 Importance of Digital Footprint

- **Online Identity and Reputation:** Our digital footprint forms a significant part of our online identity. It can influence how others perceive us, including friends, family, employers, and even strangers. A positive digital footprint can open up opportunities in personal and professional spaces, while a negative one can have adverse effects.

- **Privacy and Security Risks:** Digital footprints are a gold mine of information and can pose privacy and security risks. They can reveal personal information that might be exploited by cybercriminals for identity theft, scams, or hacking.
- **Employment Opportunities:** Many employers now research potential employees online as part of the hiring process. A digital footprint that reflects professionalism and responsibility can be advantageous, whereas inappropriate or controversial content can harm job prospects.
- **Marketing and Personalization:** Companies use digital footprints to understand consumer behaviour, preferences, and trends. This data helps in targeted advertising and personalization of services, enhancing user experience but also raising concerns about privacy and data use ethics.

4.6.3 Managing Your Digital Footprint

- **Be Mindful of Online Activities:** Regularly review and manage what you share online. This includes being cautious about posting sensitive personal information and understanding privacy settings on social media platforms.
- **Regularly Monitor Your Online Presence:** Use search engines to check what information about you is publicly accessible. This will help in understanding and managing your digital reputation.
- **Educate Yourself and Others:** Stay informed about the ways in which your data can be used and shared online. Also, educate children and less tech-savvy individuals about the importance of maintaining a positive digital footprint.
- **Secure Your Data:** Use strong, unique passwords for different accounts and enable two-factor authentication where possible. Be wary of phishing scams and unauthorized access to your personal data.

4.6.4 Protecting digital footprint

Manage and protect your digital footprint by following website safety habits practising good digital hygiene. Start with the following ways to protect your digital footprint:

- Create strong passwords and use a password manager
- Check that a website is safe before visiting
- Tighten your social media privacy settings
- Limit the amount of personal information you share online

- Delete old accounts you no longer use
- Set up Google Alerts for your name to monitor content created about you
- Use an identity protection service like AVG BreachGuard to know if your personal info is ever leaked online
- Be careful if you use the "Login with Facebook or Google" feature
- Always update your software
- Browse safely on public Wi-Fi by using a VPN.

4.7 Plagiarism

Mr Kumar had given an assignment to his students during summer vacations. All of his students submitted the assignment. All were very beautiful with full content, nice pictures and write ups. Some of the information may be used from other sources. But students were not aware that the content which is driven from different sources has to be given due credit. Then Mr. Kumar introduced to them Plagiarism.

Combining ideas or work from another source into your own work without giving due credit, either with or without the original author's permission. This includes all written works, both published and unpublished, in manuscript, print, or electronic format. It also includes the usage of writing produced entirely or partially using artificial intelligence. It is also considered plagiarism to reuse your own work without giving credit.

The necessity to acknowledge others' work or ideas applies not only to text, but also to other media, such as computer code, illustrations, graphs etc. It applies equally to published text and data drawn from books and journals, and to unpublished text and data, whether from lectures, theses or other students' essays. You must also attribute text, data, or other resources downloaded from websites.

Please note that artificial intelligence (AI) can only be used within assessments where specific prior authorisation has been given, or when technology that uses AI has been agreed as reasonable adjustment for a student's disability (such as voice recognition software for transcriptions, or spelling and grammar checkers).

4.7.1 Forms of plagiarism

- **Word for word (Verbatim) quotation without clear acknowledgement:** Quotations must always be clearly marked with quotation marks or indentation, along with complete

citation of the original sources. The reader must always be able to tell which passages are entirely your own and which ones you borrowed concepts and language from others.

- **Copy and paste from the Internet without clear acknowledgement:** Online-sourced information needs to be properly cited and added to the bibliography. All content available on the Internet should be thoroughly reviewed because it is likely to have passed the same academic peer review procedures found in sources.
- **Paraphrasing:** Paraphrasing the work of others by altering a few words and changing their order, or by closely following the structure of their argument, is plagiarism if you do not give due acknowledgement to the author whose work you are using.
- **Collusion:** This can include students working together without permission, failing to credit help they receive, or not adhering to the rules exactly when working in groups on tasks. It is your duty to make sure you understand exactly what constitutes acceptable collaboration and what portions of the work need to be completed by you alone.
- **Failure to acknowledge assistance:** You must clearly express your appreciation for all the input that has gone into the creation of your paper, including suggestions from classmates, lab techs, and other outside sources.
- **Utilizing content authored by experts or other individuals:** It is not appropriate for you to utilize outside agencies for the creation of your work or turn in work that has been created for you, even if the writer agrees. You must conduct your own research because doing so is essential to your intellectual growth and training.
- **Self-plagiarism**: It means reusing work that you have already published or submitted for a class. It can involve:
    - Resubmitting an entire paper
    - Copying or paraphrasing passages from your previous work
    - Recycling previously collected data
    - Separately publishing multiple articles about the same research

4.7.2 Plagiarism is unethical Firstly, it is unethical because it is a form of theft. By taking the ideas and words of others and pretending they are your own, you are stealing someone else's intellectual property.

Secondly, it is unethical because the plagiarizer subsequently benefits from this theft.

Thirdly, a degree is evidence of its holder's abilities and knowledge. If a student gains employment on the basis of a qualification they have not earned, they may be a risk to others.

Treat others online the way you wish to be treated.

It is easier to say hurtful or disrespectful things online, however, it is important to remember that your classmates, teachers, and friends are real people and they might get affected by your actions. It is essential to keep in mind that others can have different opinions from your own.

Chapter 5: Legal Aspect of Cyber Safety and Security

Objectives:

At the end of the session, learners will be able to:

- Define cyberspace and cybercrime
- Know about various cyber crimes related to children
- Identify the legal provisions with respect to crimes related to children
- Practice cyber safety tips to protect oneself from cybercrimes
- Know where to report a cyber crime

Outline:

- Introduction to Cyberspace and Cyber Crime
- Types of Cyber Crimes
- Information Technology Act 2000
- DPDP Act 2023
- Safety Tips for students
- Reporting Mechanism
- Steps to be taken by school if any incident of cyber crime is reported

5.1 Introduction

Shruti has recently joined a new school. She is a student of class 8 and is excited to make new friends. Following one of her classmate's suggestions, she created an account on a social media platform and made virtual friends, including some whom she did not know personally. One day,

someone posted her morphed and obscene pictures and also wrote derogatory comments. She was traumatised, but too scared to tell her parents or teachers.

What do you think Shruti should have done? Is there a provision to punish the person who had posted her morphed images and derogatory comments? Does Indian Legal System give legal relief to the victim and punishment to the criminal just as is done in case of physical crimes?

5.2 Cyber Crime and its Types

Internet enabled technology has given us a public space where anyone can post any type of information. This public space is called **cyberspace**. It is the virtual world of computers, laptops, smartphones, and/or digital devices that are connected with each other through the Internet. Any information posted in cyberspace may or may not be legally or ethically correct. The unethical behaviour, driven by greed, envy, revenge, or competition, leads to illegal activities in cyberspace. These activities, known as **cyber crimes**, are meant to harm users on the network by stealing or damaging data or causing harm to someone's reputation. In schools, the teachers post assignments, worksheets, and results on websites or social media groups. The students too interact with each other on social media platforms for personal or academic purposes. Therefore, it is crucial to understand about prevalent cyber crimes and the legal provisions for the same.

Types of Cyber Crimes

A cyber crime is an intentional act to steal, modify, damage, or destroy data or any other resource on a computer network or digital device. Some of the prevalent cyber crimes are:

5.2.1 Identity Theft

It amounts to the act of stealing personal, financial, medical or any other information of a person. This is done with an intent to commit a crime in the victim's name, make unauthorized purchases, loans or to cause any other form of financial or personal damage to the victim. Hence, one should be sure about the identity of the recipient before posting personal information, such as copies of I-cards, Aadhar cards, or any other such data online.

5.2.2 Online Harassment

Online harassment is the umbrella term for different cyber crimes that may not cause any financial loss to the victim but causes immense mental distress and trauma. It refers to the activities performed using digital devices on social networking platforms, emails or messaging services, gaming platforms, etc.

- **Cyber Bullying:** Cyber bullying is on the rise among school and college students. The victim is threatened, intimidated, humiliated, or harassed by posting derogatory comments, obscene pictures or audio-video messages. This happens to such an extent that the victim is traumatised and distressed, and sometimes develops suicidal tendencies. Legal action can be taken against the perpetrator(s) of cyber bullying.
- **Cyberstalking:** In this case, the perpetrator purposefully follows the victim online and makes repeated attempts to contact him/her through emails, text, audio, or video messages on social media platforms. He/she may also communicate with friends, families and/or employers of the victim, to spread accusations and lies. This is done to such an extent that the victim becomes uncomfortable and distressed. The victim may press legal charges against the stalkers.
- **Doxing:** Also known as dropping docs, it refers to publicly revealing or publishing private or personal information about an individual without his/her consent, typically with malicious intent. It is done with the intention to extort, intimidate, or embarrass the victim. Doxing in itself is not illegal, but it often contributes to serious criminal offences such as harassment, stalking, intimidation, identity theft, or incitement to violence.
- **Trolling:** Trolling includes posting derogatory comments on social media posts to gain attention or cause harm to the victim. Soon, other users also start posting derogatory comments and the victim becomes a target of public embarrassment. Although trolling does not invite legal action it causes mental agony to the victims leading to loss of self confidence and self-esteem.
- **Catfishing:** Catfishing is a form of cybercrime where an individual creates a fake online identity to deceive others, typically for fraudulent or deceptive purposes. This can involve creating fake social media profiles, dating profiles, or email accounts to establish relationships with unsuspecting victims. The catfisher may use stolen/morphed photos or information to make the fake identity appear convincing.
- **Excluding:** When a user is deliberately invited or excluded from a particular group, it is called excluding. The person who is excluded feels left out and lonely that disturbs him/her emotionally.

5.2.3 Financial Frauds

Financial frauds involve the use of e-transactions through net banking, UPI, eWallets, or through credit/debit/ATM cards. Most of the financial frauds happen due to the victim's error or greed. The fraudster gets hold of confidential financial information from the victim such as usernames, passwords, security pins, etc. Once this information is available, the cyber criminals are able to fraudulently transfer money to their accounts. Some of the financial frauds are:

- **Phishing:** In this case, the criminal sends a fraudulent email that seems to be coming from a legitimate source. In the pretext of locking an account by the bank, winning a lottery, or winning a prize, the email aims to extract confidential and private information such as usernames, passwords, CVV, OTP, security pins, etc. from the user. Once the user gives any of this information, it is then used to perform fraudulent transactions and cause monetary loss to the victim.
- **Vishing:** In this type of fraud, the fraudster calls the victims and lures them to give the sensitive information by phone, which is later used to commit the crime.
- **Smishing:** In this case, the victims receive text messages that lure the victims to either call back or click on the fraudulent link given in the SMS. Once they do so, their financial information is extracted and used for malicious purposes.
- **E-Commerce Frauds:** These types of frauds target online shoppers and sellers. The victims are deceived into paying for goods and services that may not exist or are not as described by the e-commerce platform, or goods and services are not received even after making online payments.

5.2.4 Crimes related to children

With the increased use of smart phones by children, their vulnerability to cyber crime has also increased. The child’s innocence, lack of knowledge, and desire to be appreciated, is exploited by malicious users. Children often access social networking websites and interact with known and unknown people. They can become victims of cyber bullying, cyber stalking, or may get exposed to sexually abusive content, hate speech, violence, etc. Children are also put at risk when the personal data is collected by companies for marketing purposes.

Child Sexually Abusive Material (CSAM) is any type of digital material that contains sexual images of a child who is abused or sexually exploited. Such type of material depreciates the mental and physical health of children as they might face shame, embarrassment, and guilt. Other than cyber bullying and cyber stalking, other common crimes related to children are:

- **Cyber Grooming:** In this type of crime, an unknown adult befriends a child online to gain his/her confidence. Thereafter, the criminal pressurises him/her for sexual favours, extract personal information of their parents and family members, and later use the same for committing crimes. Sometimes, the child may be forced or lured to meet the criminal personally without informing anyone.
- **Online Sextortion:** It involves blackmailing the child. The criminal threatens to disclose sexually explicit images of the victim on social media, if he/she does not provide give online or offline sexual favours, or pay some amount of money. This coercion can result in mental agony, socio-cultural loss, and distress for the child.
- **Sexting:** In this type of cyber crime, the sexually explicit text, images, audio-video content, emails, etc. are shared with children.
- **Child Pornography:** Creating or sharing of any type of CASM material among children or adults is child pornography, and is strictly prohibited.

5.2.5 Hacking

Hacking is one of the most common forms of cybercrime. The persons who commit the crime of hacking are known as hackers. They gain unauthorised access to systems or networks to cause data theft, system disruptions, injection of malware or any other type of harm to the individual or an organisation.

5.2.6 Data Breach

Data breach occurs when any information is accessed from any device or network without proper authorization. Generally, a data breach is done by the employee or a person aware of the company's databases. The data may be sold to dark web or rival companies in exchange for money or any other favour.

5.2.7 Misinformation

This is an act that involves spreading false information with an intent to misguide or mislead the online users. This may or may not be done intentionally but can have negative consequences for society, at large.

5.2.8 Misuse of deepfake technology

Deepfake technology can make any virtual person as real or vice versa, saying or doing anything. Multiple apps for creating deepfakes are easily available on the Internet. Its proliferation in 2023 contributed to the spread of a lot of misinformation/disinformation across the world. Some of

these fakes were used for political purposes while others were for creating pornographic and entertainment content. This led to social turmoil, political instability, and in some cases, financial damages. The lack of technical and remedial measures about the same added difficulties in detection and prevention of such synthetic content. As of now, there is no specific legal provision that deals with deepfake, but governments are in the process of framing rules, regulations, and laws to curb them.

5.3 Laws and Acts to Protect from Cyber Crimes

5.3.1 Children's Online Privacy Protection Rule (COPPA)

The law enforces that the websites or online services, collecting personal information of children below the age of 13 years, must obtain parental consent before doing so. This is to ensure safety and privacy of children in the digital world.

5.3.2 Information Technology(IT) Act 2000

Do you think that the Internet is a double-edged sword for children? It gives access to all forms of information, but it also provides potential exposure to harmful and age inappropriate content. The increasing number of children using social media, online gaming and other platforms for sharing images, audio and video has forced the government and child care agencies to monitor the online activities related to children.

The IT Act 2000 plays a crucial role in protecting the rights and safety of all online users, especially children. In case of any cybercrime or online harassment, the IT Act provides a legal framework for children to seek recourse. The table given below provides information about some of the common sections, offences and punishments as laid down in the act:

Table 1: Offences and Punishments in IT ACT 2000

Section	Offence	Punishment	Example
43	Downloading the data which leads to malware, ransomware, or DOS attack.	Penalty up to one crore.	Sarah, receives an email from her company's IT department, instructing her to update her software. She clicks on the provided link, unknowingly downloading ransomware onto her computer that encrypt/damage her data.
65	Tampering with Computer Source Documents	Imprisonment up to 3 years or fine up to Rs 2 lakhs	Reddy modifies the code of a school competition program and tampers game scores so that his team could win.
66	Computer Related Offences such as hacking	Imprisonment up to 3 years or fine up to Rs 5 lakhs	• Tony hacks into the school's computer system to change his grades. • Mouli bullies classmates online and spreads rumours through fake accounts.
66-A	Sending offensive messages through communication and digital devices.	Imprisonment up to 3 years and fine	Jatin is a young professional who loves to play online games with his friends and colleagues. In order to discourage his opponents and make them nervous , he sends messages undermining their playing prowess and at times he also uses abusive and offensive words.

Section	Offence	Punishment	Example
66-B	Dishonestly receiving stolen computer resource or communicatio n device	Imprisonment up to 3 years and/or fine up to Rs. 1 lakh	Sukhwinder was given a pen-drive by his friend, that actually belonged to their class teacher. It contained confidential data. He did not inform his teacher about it, instead starting searching for question papers files..
66-C	Identity Theft	Imprisonment of either description up to 3 years and/or fine up to Rs. 1 lakh	For her 18th birthday, Parul planned a party. She posted an invite with her picture, address, contact number, venue, time and date of party on her social media accounts. A malicious user stole her identity and formed a fake profile. Thereafter, he started posting offensive images from the fake id.
66-D	Cheating by impersonation by using computer resource	Imprisonment of either description up to 3 years and /or fine up to Rs. 1 lakh	Rishi created a fake account of a tuition teacher on the pretext of giving free tuition. Actually, he coerced the children to post sexually offensive images.
66-E	Violation of Privacy	Imprisonment up to 3 years and /or fine up to Rs. 2 lakh	The personal information collected by online gaming applications and share with advertisers & third parties for monetary gains.

Section	Offence	Punishment	Example
67	Publishing or transmitting obscene material in electronic form	On first conviction, imprisonment up to 3 years and/or fine up to Rs. 5 lakhs. On subsequent conviction imprisonment up to 5 years and/or fine up to Rs. 10 lakh	Kannan, a disgruntled former employee, decides to seek revenge against a colleague, Jordan. Kannan maliciously and secretly obtains intimate photos from Jordan's private social media account without consent. Subsequently, Kannan creates a fake account on a public forum and publishes the explicit images, some of them morphed, along with defamatory remarks about Jordan.
67-A	Publishing or transmitting of material containing sexually explicit act, etc. in electronic form	On first conviction imprisonment up to 5 years and/or fine up to Rs. 10 lakhs. On subsequent conviction imprisonment up to 7 years and/or fine up to Rs. 10 lakh	A student shares pornographic images and videos on a class group.
67-B	Publishing or transmitting of material depicting children in sexually	On first Conviction imprisonment of either description up to 5 years and/or fine up to	A shopkeeper sexually exploited a child and filmed the act. He then sold the same on the dark web and also shared with his friends.

Section	Offence	Punishment	Example
	explicit act etc., in electronic form	Rs. 10 lakh On Subsequent Conviction imprisonment of either description up to 7 years and/or fine up to Rs. 10 lakh	

5.3.3 Digital Personal Data Protection (DPDP) Act 2023

The DPDP Act 2023 aims to protect the rights of individuals to protect their personal data and the need to process such personal data only for lawful purposes. The act applies to both online and digitised offline data. The Act also regulates the optimum and lawful use of personal data collected by organisations. The personal data that is in public domain is excluded from the scope of this act. The key highlights of DPDP Act 2023 are:

- A proper agreement should be signed between the organisation and the individual(s) whose data is being collected.
- Implement technical and organisational measures to safeguard personal data of their clients/customers.
- Implement a grievance redressal mechanism for handling queries from any person related to the organisation.
- Irrecoverably delete personal data after the purpose for which it was collected has expired.
- Notify personal data breaches to the Data Protection Board and affected individuals.
- Cross border transfer of data is valid until certain transfers are explicitly restricted by the government.

5.4 Cyber Safety Tips for Students

- Be respectful to other online users.
- Do not open suspicious emails and/or take suspicious phone calls.

- Use strong passwords.
- Do not click on ad pop-ups or on any suspicious links.
- Never leave your devices unattended, especially if you are logged in to any application
- Always use original and updated software and antivirus
- Back up your data on a regular basis.
- Always opt for Two -Factor Authentication.
- Download software from authenticated websites/play stores
- Browse secure websites
- Use Parental controls on device usage
- Do not perform any sort of financial transactions on any public network.
- Never share your personal and confidential information such as usernames, passwords, OTP, CVV, etc. with anyone.
- Check your privacy settings on regular basis
- Do not make friends with strangers online
- Do not forward or post false information

5.5 Reporting Mechanism

As discussed before, any cyber crime adversely affects the victim's mental, emotional, and/or financial health. That is why various legal provisions are laid down to help the victims and punish or deter the criminals. Depending on the nature of the crime, there may be civil or criminal remedies. In case of civil remedies, injunction, restraint orders, blocking of websites, applications or services may be sought. To seek criminal remedies, a case will be registered by the cyber crime police if the offence is cognisable. For a non-cognisable offence, a complaint has to be filed with a metropolitan magistrate. For some offenses, both civil and criminal remedies may be sought.

What should be the first step that a victim of cyber crime should take? Where should he/she report?

A cyber crime can be reported by any of the following means:

- Approaching the nearest cyber police station to report the crime.
- Calling the universal helpline number to report cyber crime in India, that is **1930.**

- Registering a complaint on the **National Cyber Crime Reporting Portal** (www.cybercrime.gov.in) . This is the official website of the Ministry of Home Affairs of Government of India for reporting any type of cyber crime. You can register a complaint on this portal under any of the three categories - Women/ Child Related Crime, Financial Fraud, and Other Cyber Crime

Figure: National Cyber Crime Reporting Portal (www.cybercrime.gov.in)

However, the procedure of reporting and evidences required vary for different types of cyber crimes:

Financial fraud

In case of a financial fraud, following steps should be taken immediately:

1. Call the helpline number of the concerned bank and block your bank account or credit/debit/ATM card. Make sure that you have all the evidence ready before you make the call. It is very important to make sure that the call centre number is verified from the official website of the bank, passbook given by bank or an official SMS message received from the bank.
2. Change the passwords of all net banking, financial, or e-commerce accounts.
3. Report the matter by either calling at Cyber Crime Helpline Number, **1930**, or by going to the nearest police station, or reporting online at www.cybercrime.gov.in. On the online portal, click **Register a Complaint** tab and select the **Financial Fraud** option. You will be asked to fill in your personal details such as Name, Address, email ID, contact

number, etc. Thereafter, you will have to give details of the crime. Make sure that you have all relevant information such as date and time of crime, UPI IDs of fraudulent transactions, your bank account numbers, exact amount of money that was fraudulently transacted, and screenshots of chats/calls/messages that lead to the cyber crime.

After you have registered your complaint, keep the copy of the complaint safe with you. You may follow up using the complaint number given to you.

Women/Child Related Crimes

According to a recent survey, children in India are exposed to online risks more than in any other country. So, it is all the more important to safeguard our children and make them secure.

The cyber crimes dealing with women and children have to be dealt with sensitivity and care by all stakeholders. That is why these type of crimes can be reported anonymously. The Indian legal system gives full right of anonymity and protection to the victim and minor witnesses as well. In child sexual harassment/ pornography, reporting is mandatory. The victim of cyber crime should follow the steps given below:

1. Take screenshots of derogatory messages, chats, indecent or morphed images or videos.
2. Block the caller/sender. It is also advised to select the **Block and Report** option so that the sender/caller is blocked and matter is reported to the service provider as well.
3. Change the password of your social media accounts. If possible, change usernames or freeze them. The social media network should be informed so that any network objectionable content can be removed in 24 hours.
4. Report the matter by either calling 1930, by reporting at the nearest police station or by registering the complaint on the National Cyber Crime Reporting Portal.

Other frauds

Other than financial and women/child related frauds, other frauds such as data breach, espionage, website defacement, malware attack, impersonation, identity theft, spamming, etc. should also be reported by using any of the methods given in the module.

Steps to be taken by school if any incident of cyber crime is reported by any student/parent:

1. Take the child into confidence and comfort him/her, so that he/she can report the matter with precise details. The identity of the victim and the student who is reporting should be kept secret.
2. The Principal should preferably, form a committee to inspect the reported matter, with at least two teachers.
3. Inform the parents of the victim. Refer the child to school counsellor or psychologist for after care support.
4. Collect evidence from social media and also by talking to students, teachers, or any other person connected with the matter.
5. Take advice from a cyber law expert.
6. If the matter is of grave concern, report the matter to the nearest police station or register a complaint on www.cybercrime.gov.in
7. Keep a complaint box, introduce e-clubs for cyber awareness, and conduct regular workshops for students, parents, teachers, administrative, and support staff of the school.

In conclusion, the legal framework surrounding cyber safety highlights the importance of protecting individuals, especially children, from the numerous threats posed by cyber crimes. With the increase in reliance on digital technologies, the risks of online exploitation, harassment, and misinformation have become increasingly prevalent. However, laws such as COPPA, the IT Act 2000, and the DPDP Act 2023 provide essential safeguards and recourse mechanisms to address these challenges. Furthermore, proactive steps such as cyber safety education, robust reporting mechanisms, and school interventions play a crucial role in fostering a safer online environment for all. By prioritizing awareness, prevention, and support, stakeholders can collectively work towards mitigating the impact of cyber crimes and promoting digital well-being in society.

Reference

Kaur, K., Gurnani, B., Nayak, S., Deori, N., Kaur, S., Jethani, J., Singh, D., Agarkar, S., Hussaindeen, J. R., Sukhija, J., & Mishra, D. (2022). Digital Eye Strain- A Comprehensive Review. *Ophthalmology and therapy*, *11*(5), 1655–1680. https://doi.org/10.1007/s40123-022-00540-9

Balhara, Y. P. S., & Anwar, N. (2019). BehavioR: a digital platform for prevention and management of behavioural addictions. *WHO South-East Asia journal of public health*, *8*(2), 101–103. https://doi.org/10.4103/2224-3151.264854

Balhara, Y. P. S., & Singh, S. (2019). Online course on basics of management of behavioral addictions involving use of internet: Observations from the first batch of participants. *Asian journal of psychiatry*, *44*, 1–3. https://doi.org/10.1016/j.ajp.2019.07.013

Computer ergonomics: How to protect yourself from strain and pain. Computer Ergonomics: How to Protect Yourself from Strain and Pain | University Health Service. (n.d.). https://uhs.umich.edu/computerergonomics

The Trustees of Princeton University. (n.d.). *Ergonomics & Computer Use | University Health Services*. Princeton University. *https://uhs.princeton.edu/health-resources/ergonomics-computer-use*

Ergonomics guidance for mobile devices - stanford university. (n.d.). *https://www-group.slac.stanford.edu/esh/medical/ergo/ergomobileguide.pdf*

Effects of smartphones on our fingers, hands and elbows. The Orthopaedic Institute. (2022, July

4). https://www.toi-health.com/physician-articles/effects-smartphones-fingers-hands-elbows/