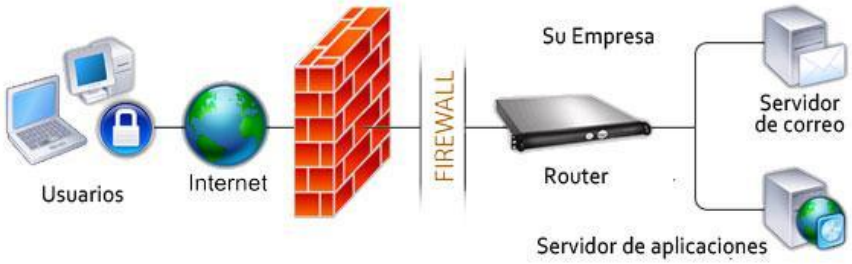
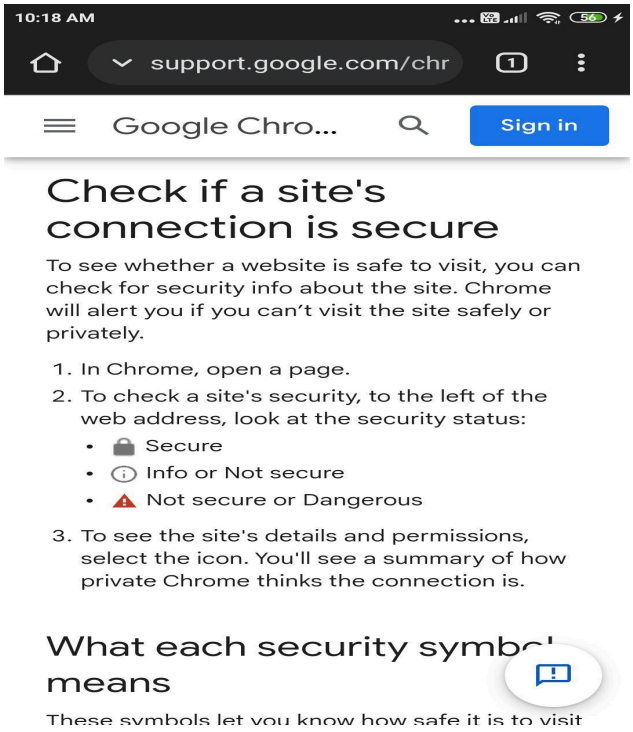
CHAPTER-15 CYBER SAFETY

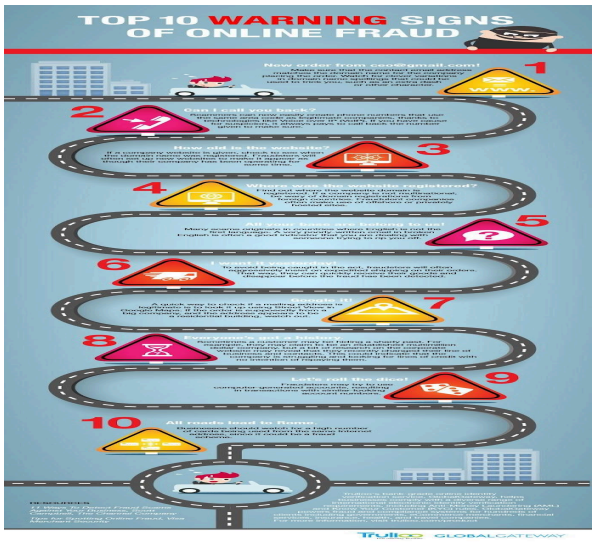
Introduction	• What is Cyber Safety • Safely Browsing the web • Identify Protection While using internet • Confidentiality of information • Cyber Crime • Computer Forensics • Cyber Law and IT ACT • Common social network Sites • Appropriate usages of Social Networks
What is Cyber Safety	Cyber safety refers to the safe and responsible use of the internet to ensure safety and security of personal information and not posing threat to anyone else's information. Cyber safety
Safely Browsing the Web	• What are the possible dangers. • How to avoid this. • How to Virtually conduct yourself while browsing .
Identity protection while using internet	Identity theft is a type of fraud that involves using someone else's identity to steal money or gain other benefits . Online identity theft refers to the act of stealing someone personal information, some is name login details and then posing as that person online.
Multiple forms of identity theft	• Financial identity theft • Criminal identity theft • Medical identity theft
	Q1.The type of root that involves using someone as an identity online is called …… . Answer- Identify theft Q2. ……refers to the safe and responsible use of the internet. Answer-Cyber Safety
Many ways website track you	• IP addresses-IP address is a unique address of your device when you're connected to the internet. it is likely that your computer shares your IP address with the other network

	device in your house or office. from your IP address of the website can determine you rough geographical location . • **Cookies and tracking scripts.** cookies are small text files on your computer is storing a small piece of information related to your online habits I. First Party cookies- These are the cookies that store your login ID password autofill information as 17 for some website that you frequently visit .
	ii.Third Party cookies -These are the cookies that websites know about search history and web browsing history so as to place advertising as per your interest.
	iii Super Cookies-Super keys are also cookies but these are persistent cookies they come back even after you delete super cookies, store cookies start and multiple places. • HTTP Referer-When you click a link your Browser load the web page link to it and tell the website where you came from . • User Agent-Your browser also send the user agent every time you connect to a website this tells the website your browser and operating system providing another piece of data that can be stored and used to target ads.
Private Browsing and Anonymous Browsing	
	

<table>
<tr><td>15.4.2.2 Private Browsing and Anonymous Browsing</td><td></td></tr>
<tr><td>Anonymous Browsing</td><td>Anonymous browsers allow user to view websites without revealing any personal information of the user like their IP address machine type location etc .</td></tr>
<tr><td></td><td></td></tr>
<tr><td>Private Browsing</td><td>Incognito browsing Open some version of the browser that will not track your activity. it particularly useful if you are entering sensitive data Like bank details into the browser as it can minimize the risk of your information being saved to the computer .</td></tr>
<tr><td></td><td>Proxy- Works By acting as a middleman between your computer and the website you want to access. now the tracking website will get the IP address information that belongs to the proxy site so you are effectively getting the same content from another source without it getting to know your browsing details</td></tr>
<tr><td></td><td>Virtual Private Network(VPN) -VPN is a method used to add security and privacy to private and public networks like Wi-fi, Wi-Fi Hotspot and the internet. VPNs are most often used by corporations to protect sensitive data .</td></tr>
<tr><td>15.5 Confidentiality of Information</td><td>Information
Public post,pictures ,comments,views,credit card details,mail id,phone no,password,social accounts id
<table><tr><td>Public</td><td>Private</td></tr><tr><td>Public st,comments,views,social accounts id.</td><td>Credit card details,mail id,phone no,password</td></tr></table></td></tr>
<tr><td>Practices to ensure the confidentiality of information</td><td></td></tr>
<tr><td>Use firewall wherever possible</td><td>You system must be secured such that only authentic users can connect to it. Firewall is good solution for it. Firewall is a program that monitors all communications and Trap all illicit packets</td></tr>
</table>

	 **Go to Start and open Control Panel. Select System and Security > Windows Defender Firewall. Choose Turn Windows Firewall on or off. Select Turn on Windows Firewall for domain, private, and public network settings.**
Control browser setting to block tracking	**To minimize threats you can turn your default browser setting to exclude cookies, especially third party cookies since they can be used to build up detailed profiles of your surfing patterns over time .**
Browse privately wherever possible	**DuckDuckgo** **A secure URL should begin with “https” rather than “http.” The “s” in “https” stands for secure, which indicates that the site is using a Secure Sockets Layer (SSL) Certificate. This lets you know that all your data is encrypted as it passes from your browser to the website's server.**
Be careful while posting on internet	
Ensure safe sites	

while entering crucial information	**A secure website's URL should begin with "https" rather than "http". The "s" at the end of "http" stands for secure and is using an SSL (Secure Sockets Layer) connection. Your information will be encrypted before being sent to a server.** 
Carefully handle emails	**www.facebo0k.com**
Do not give sensitive information on wireless networks	
Avoid using public computers	
15.6 Cyber Crime	**Cyber crime is any criminal offence that is fascinated by or involves the use of electronic Electronic Communication or information systems including any electronic device computer or the internet.** **In general form it covers like phishing, credit card for fraud, illegal downloading, industrial espionage ,cyber bullying cyber stalking, cyber terrorism, creation and or distribution of virus and spam.**
15.6.1 Cyber Trolls and Bullying	**Cyber trolls are Derogatory messages or comments posted online targeting people .**
15.6.2 Cyber Bullying	**Harassing,embarrassing, defaming using modern techniques Technologies like the internet ,cell phone , messenger social networks is called cyber Bullying.**
15.6.3 Cyber Stalking	• **They collect all personal information about the victim such as name, family background ,telephone number of Residence and workplace ,daily routine of the victim, address of the residents and place of work .** • **They may post this information for any obscene or illegal website as if the**

	victim is posting . • Pupils of all kinds from Nook and corners of the world who come across this information start calling the victim at his/her residence .
15.6.4 . Spreading Rumors Online	
15.6.5 Online Fraud	• Non delivered goods • Non existent companies • Stealing information' • Fraudulent payments 
15.6.6 Information Theft	
15.6.7 Scams	
15.6.8 illegal Download	
15.6.9 child pornography	
16.6.10 Reporting Cyber Crime	Cyber Crime Portal
Computer Forensics	What interpretation of computer media or Digital evidence.

Cyber Law and IT Act	**Cyber law is important because it touches almost all aspects of transactions and activities on and concerning the internet.**
India IT Act and IT(Amendment)Act 2008	**Information Technology Act 2000(IT ACT 2000)** **2008-Security of data ,Cyber Terrorism** **1.Digital Signature-** **2. Electronic Governance-** **3.Offence and Penalties- Maximum penalty for any damage to computers or computer systems is 1 crore** **4.Amendments to other law**
Common Social Network Sites	**1.Facebook** **2.Twitter** **3.Linkedin** **4.Instagram**
Appropriate Usage of Social Network	**Digital footprint** **Digital footprints are the record and traces of individual activity is the use of internet digital footprints are permanently stored.** **Digital footprints are the record and traces individuals leave behind as the use the internet .** **Active footprint-Which are formed by your online activity you do knowingly** **Passive Digital footprint- Which are formed by any and every activity that you perform online and you do not even know about it. online payments games you play and show on.**
Privacy Setting	**Account setting** ● **Who all can see what you have posted.** ● **Who all can send request to you** ● **All information about you is visible to others, even to your contacts etc.**
Social media	**1.Be authentic**

Étiquettes	**2.Be secure- Create a strong password.** **Frequently changing your password.** **Not using the same password over multiple social media accounts .** **Never share your personal credentials like username and password with others .** **Identify fake information ,post, fake news and never to trust them.**
	3. Be Reliable-If you are associated with an institution or Organization in some form and you are sharing your personal view about something use our disclaimer to make it clear that this is your personal view and you do not represent any institution or organization here.
	4.Don't Pick Fights Online-Sometime people may respond to your post and you do not find good. In such a case it is advised not to pick fights online. rather convey your unhappiness through constructive post /messages while carefully choosing the right words.
	5. Don't Use a Fake Name-Never pretend to be someone as if you think that making an anonymous profile would hide you online you are mistaken.
	6.Protect your Identity-While you should be honest about yourself but you should never provide or post personal information online.
	7.Does your information/Post Pass the Publically Test-Before you post something online perform publicly test on it the rule is if your post message is not acceptable for face to face conversion over the telephone or in other phone another medium then it is not acceptable for a social media site
	8.Respect you audience- sometimes school college students talk in slang or you some abusive word which they find ok with within their small group but this thing must not be posted online .
	9.Respects othe's Sentiments-You should always respect others privacy

	and be considerate for topics that may be concerts and States such as Pol politics and religion.
	10.Monitor Comments-Most people who maintain social media sites welcome comments that build credibility and community. You should prefer to review and approve comments before posting them on your site.
Execrcise Questions	Q1. What makes your online identity ?
	Answer-
	Q2.What are cookies
	Answer
	Q3. What are super cookies?
	Q4. What is private browsing ?
	Q5. Can you see history of pages you visited in private browser window
	Q6. Posting something which you just heard or received but you are not sure of its authenticity is a crime.
	Q7 Which of the following is not an example of cybercrime. i. Stealing computer hardware ii. cyber bullying iii. cyber stalking iv. stealing someone's online identity
	Answer-
	Q8.When a person is harassed repeatedly by being followed ,called or be

	written to he/she is a target of I. phishing ii. Cyber Stalking iii.Identity theft iv.Plagiarism
	Answer-
	Q9.What is meant by the term cybercrime i. Any crime that uses computer to jeopardize or attempt to jeopardize national security ii. the use of computer networks to commit financial or identity fraud iii. the theft of Digital information iv. Any crime that involves computers and networks .
	Answer-iv. Any crime that involves computers and networks .