

CYBER Safety

HANDBOOK FOR STUDENTS OF SECONDARY & SENIOR SECONDARY SCHOOLS





भारत

Cyber Peace
Foundation

Year of Publication: 2020
CBSE in collaboration with Cyber Peace Foundation



ACKNOWLEDGMENT

Patrons:

Sh. Ramesh Pokhriyal 'Nishank', Minister of Human Resource Development, Government of India.

Sh. Sanjay Dhotre, Minister of State for Human Resource Development, Government of India.

Ms. Anita Karwal, IAS, Secretary, Department of School Education and Literacy, Ministry of Human Resource Development, Government of India.

Advisory, Editorial and Creative Inputs:

Our gratitude to Ms. Anita Karwal, IAS, for her advisory, editorial and creative inputs for this Manual during her tenure as Chairperson, Central Board of Secondary Education (CBSE).

Mr. SN Pradhan, IPS, Director General, National Disaster Response Force (NDRF).

Sh. Anurag Tripathi, IRPS, Secretary, Central Board of Secondary Education (CBSE).

Dr. Antriksh Johri, Director(Information Technology),Central Board of Secondary Education (CBSE).

Dr. Joseph Emmanuel, Director(Academics),Central Board of Secondary Education (CBSE).

Dr. Biswajit Saha, Director(Skill Education& Training),Central Board of Secondary Education (CBSE).

Sh. Rakesh Maheshwari, Group Coordinator, Cyber Laws and e-Security, Ministry of Electronics and Information Technology (MeitY).

Dr. Debarati Haldar, Professor, Legal Studies, Karnavati University.

Dr. Manoj Sharma, National Institute of Mental Health and Neurosciences (NIMHANS).

Dr. Rachna Bhargava and Dr. Rajesh Sagar, All India Institute of Medical Sciences (AIIMS).

Dr. HK Kaul, Developing Library Network (DELNET).

Value adder and Co-ordinator:

Dr. Praggya M. Singh, Joint Secretary (Academics), Central Board of Secondary Education (CBSE).

Capt. Vineet Kumar, President, Cyber Peace Foundation.

Content Developed and Curated by Cyber Peace Foundation:

Ms. Neelam Singh | Ms. Karuna Bishnoi | Ms. Janice Verghese | Ms. Akanksha Kapur | Mr. Kumar Vikram | Ms. Aditi Pradhan
Ms. Dhruvi Shah | Ms. Jemisha Bhalsod | Ms. Ayushi Shukla

CONTENTS

INTRODUCTION 1

01 DIGITAL ACCESS 4

02 DIGITAL LITERACY 9

03 DIGITAL COMMUNICATION 15

04 DIGITAL COMMERCE 24

05 DIGITAL ETIQUETTE 29

06 DIGITAL HEALTH AND WELLNESS 42

CONTENTS

07 DIGITAL RIGHTS, FREEDOMS AND RESPONSIBILITIES 49

08 DIGITAL SECURITY 55

09 DIGITAL LAW 72

USEFUL CONTACTS 82

USEFUL RESOURCES 83

ANSWERS 84

INTRODUCTION

Technological advances are changing the world in ways that could not have been imagined. The emergence of advanced digital innovations are providing new opportunities to connect and learn, and have begun influencing every aspect of human life.

Children and young people have shown greater ability to adapt and adopt digital devices and innovations, which augurs well for the future. They use the devices and apps for a variety of functions, including self-expression, communication, networking, research, entertainment, and much more. The internet has enabled children to become active social agents and to mobilise for social, ecological and other causes. They are increasingly able to project their voices with unprecedented reach.

However, an assumption is often made that young people have superior skills with digital technology, which surpass those of their parents and teachers.

It may or may not be right. Many young people are confident in using a wide range of technologies and often turn to the internet for information. They seem able to learn to operate unfamiliar hardware or software very quickly and may take on the role of teaching adults how to use computers and the internet. But the confidence with digital technology can also be misleading.

Many of them frequently struggle when applying them to research tasks. They can find it difficult to work out whether information on an unfamiliar website is trustworthy, and rely on their chosen search engine's rankings for their selection of material. They may not understand how search terms work or of the powerful commercial forces that can result in a particular company being top of the search engine's list. They may not be aware of the lurking risks and threats and the fact that some of their actions can invite them trouble.

Furthermore, the digital skills and knowledge are not evenly spread amongst all young people. Dearth of research on the subject has prevented a nuanced analysis of who are most likely to lag behind in the opportunities afforded by technological advances. However, there is general agreement among those working on cyber safety and security among children and young people that gender is a major impediment.

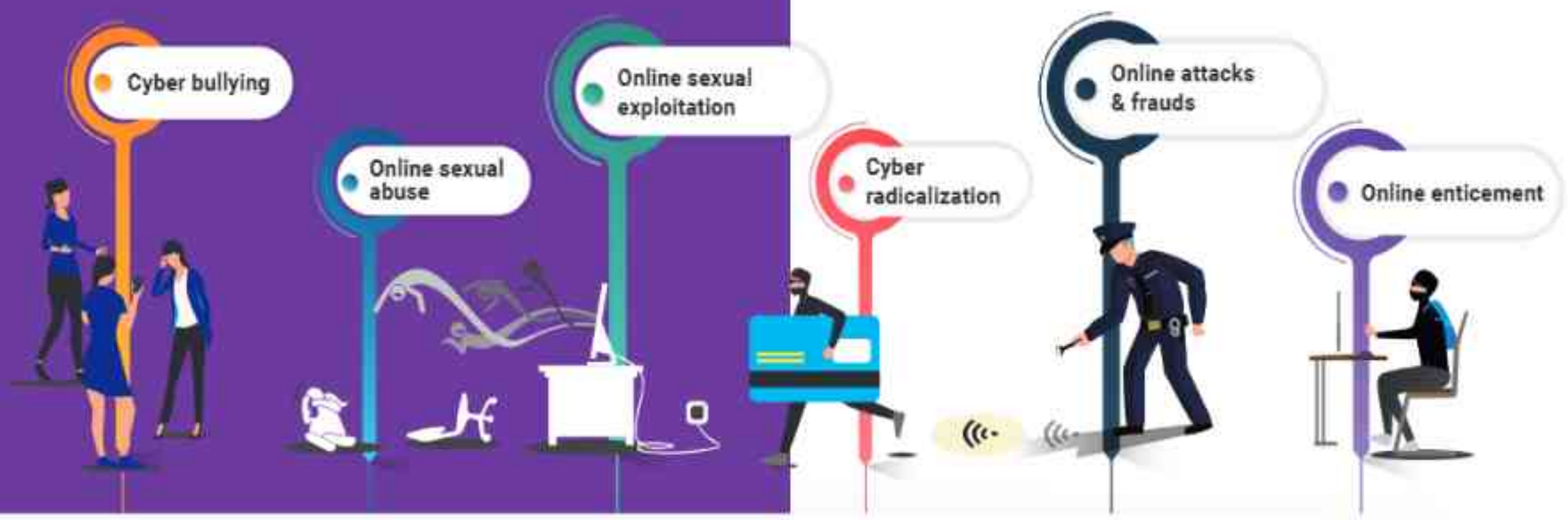
Social norms have impeded girls' access to opportunities, including the access and use of digital devices and the internet. Many of them belonging to socially or economically marginalised families in rural, semi-urban and urban areas have either no access, or limited, or supervised access to digital technologies, which could enable them to exercise their agency, autonomy and rights in an increasingly interconnected world.

The exploration of new vistas and acquisition of rich experiences online require a strong element of caution. After all, every light has its shadow. The technologies can be misused or overused in ways that are detrimental to the users and even non-users.

UNICEF in its Child Online Protection in India report in 2016 had presented the following typology of risks and threats



Figure 1: Manifestations of child online threats, abuse and exploitation in india



GROOMING

- Emotional harassment
- Defamation & exposure
- Imtimidation
- Social exclusion
- Sexual harrassment
- Production and consumption of child sexual abuse materials
- Sexual solicitation
  Aggressive sexual solicitation
- Blackmail and financial extortion
- Commercial sexual exploitation and trafficking
- Ideological indoctrination and recruitment
- Threats or act of extreme violence
- Attacks on devices: malware infection
- Exposure to inappropriate content: Pharming
- Identity theft: phishing, hacking, privacy breach
- Malvertising
- Producing and consuming pirated music and videos
- Financial fraud
- Enticement to drug trafficking
- Harmful behaviour: exposure to inappropraite content, Access to alcohol and drugs
- Illegal behaviour: cheating plagiarism, gambling, drug trafficking
- Self-harm: sexting, self-exposure

Source: UNICEF India Report

The above classification presents a birds' eye view of the risks and threats which contribute to the vulnerability of children and young people in the digital age. The other side of the coin is resilience among them, which needs to be nurtured and strengthened in order to empower them for the challenges and opportunities introduced by digital technologies.

The optimal safeguard for children is to facilitate their access to the internet, protect their privacy, encourage self-expression, and ensure that they can recognise potential dangers and know what to do about them. The concept of digital citizenship has emerged as a useful framework of various facets that need to be developed and strengthened.

Basically, there are nine elements of digital citizenship

01

Digital Access:

Equitable distribution of technology and online resources is an important issue from the perspective of human rights and social justice.

02

Digital Literacy:

Understanding technology and its use is the basic condition for optimising its benefits.

03

Digital Communication:

The electronic exchange of information with other people, through emails, cell phones and instant messaging, constantly and without delay.

04

Digital Commerce:

Increasing buying and selling of goods and services has opened vistas for the sellers, service providers, and consumers.

05

Digital Etiquette:

Digital etiquette describes the norms or appropriate and responsible behaviours while using technology devices.

06

Digital Health and Wellness:

Digital well-being is balancing your online and offline lives and using tools efficiently to make the most of technology and the internet.

07

Digital Rights, Freedoms and Responsibilities:

A collective sense of rights and responsibilities is important in a digital society for maintaining social harmony.

08

Digital Security:

Awareness of potential online risks, threats and attacks and the ways and means of preventing them are important skills to have in an interconnected world.

09

Digital Law:

At the core of digital citizenship are basic ethics, which are reflected in national and international laws.

01 DIGITAL ACCESS

1.1 WHAT IS DIGITAL ACCESS?

The telecom market is very competitive with various mobile companies trying to offer the best and cheapest plans which has led to the world's cheapest mobile data packs being offered in India. A study conducted across 230 countries over a period of one month found that Indians pay an average of Rs 18 for a gigabyte of data compared to the global average of Rs 600. The internet usage in India has exceeded half a billion people as of December 2018. The usage is equal for both rural and urban India with mobile phones being the primary source to access the internet.

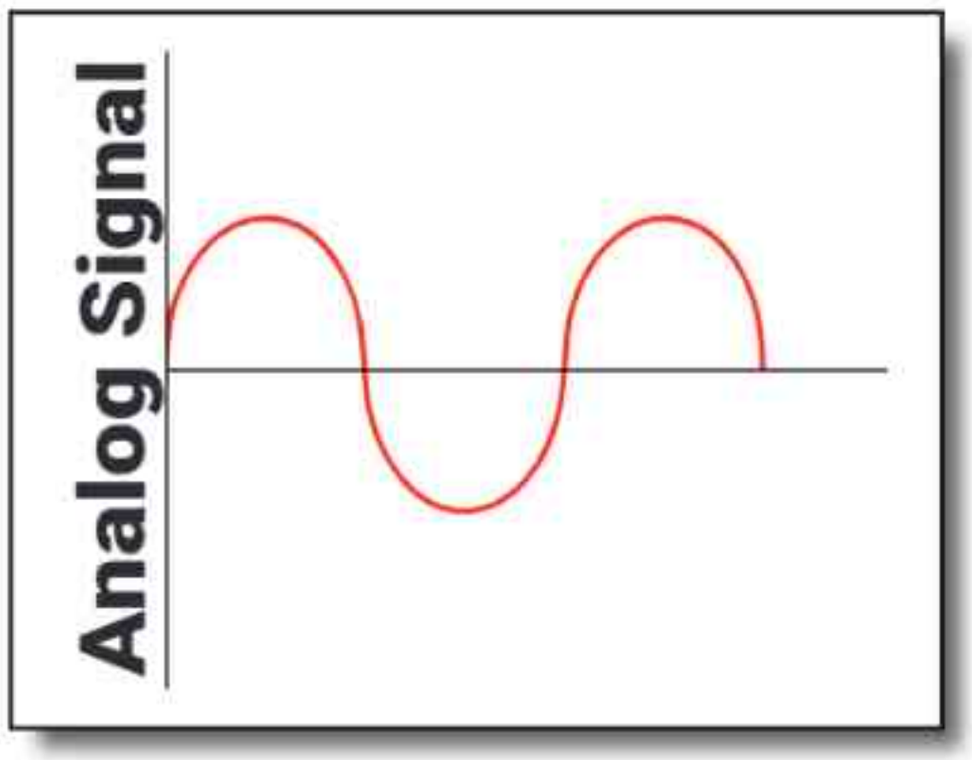
1.2 NEWER VISTAS WITH DIGITAL DEVICES AND INTERNET

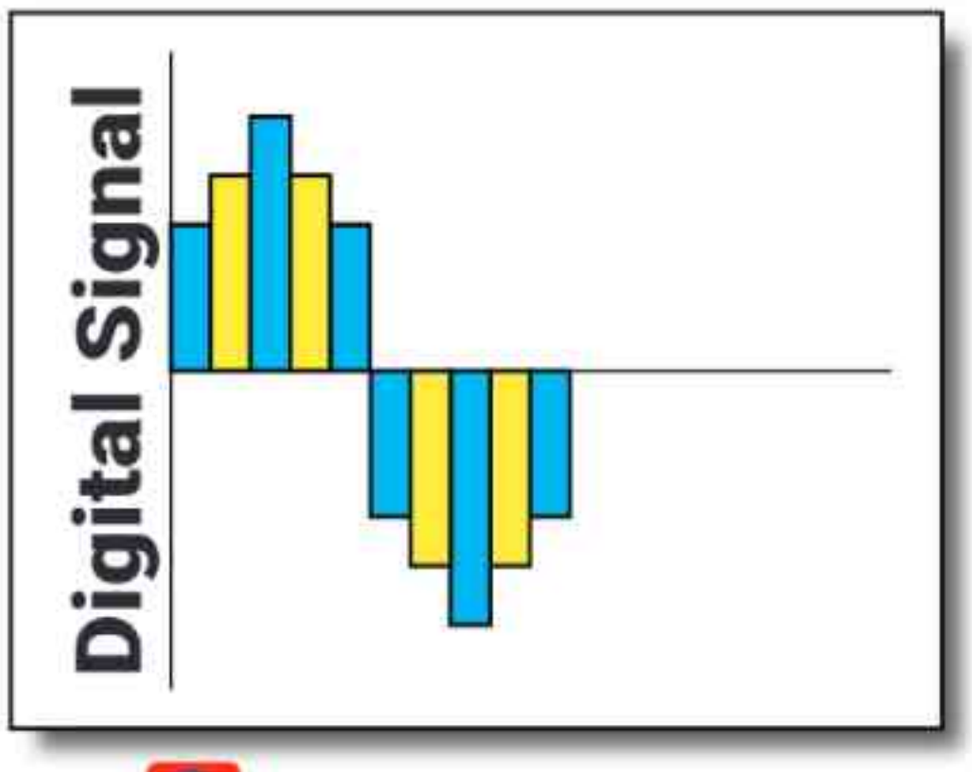
Technological innovations can be seen everywhere, in our homes, classrooms and in our surroundings too. The following categories of devices perform different but interlinked functions.

a) Mobile phones, desktop and laptop computers, tablets
b) E-readers, e.g., Kindle.
c) Dongle and Wi-Fi router.
d) Internet connected printer.
e) Internet Of Things (IoT) Devices: Smartwatches, Smart TV, Smart refrigerators, home assistants (e.g., Alexa, Google Home and Siri).
f) Whiteboards and smart boards in smart classrooms.

These innovations have made lives easier than ever, but misuse and exploitation can lead to unanticipated risks. The Internet is an interconnection of networks that uses internet protocol to link devices worldwide. With digital devices and access to the internet, several functions can be performed quickly and simultaneously. For instance: sending and receiving email, using social media, watching movies and television series, accessing large open information library from millions of websites, and writing blogs.

Digital technology is primarily used these days with new physical communications media, such as satellite and fibre optic transmission. A modem is used to convert the digital information in the computer, mobile phone, and other such devices to analog signals for the phone line and to convert analog phone signals to digital information for the computer.







1.3 NAVIGATING THE CYBERSPACE

Internet And The World Wide Web

The internet may be considered as a vast network that enables an individual to obtain any kind of information available. "The world wide web, commonly known as www, is one of the most used legitimate platforms to navigate using search engines like Google, Yahoo, Bing and DuckDuckGo. This is just the tip of the iceberg."

A Minute on the Internet in 2019

Estimated data created on the internet in one minute

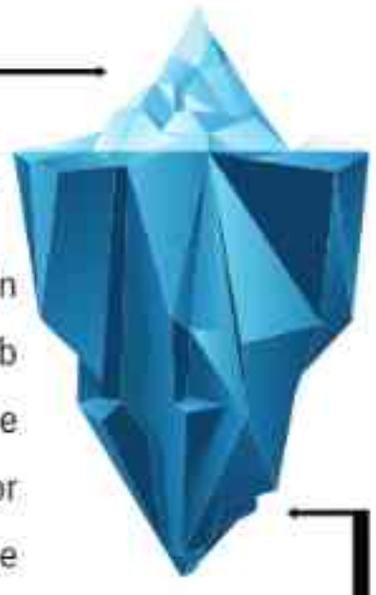
https://www.statista.com/chart/17518/internet-use-one-minute/



The No Go Zone: Deep Web And Dark Net

Public

Frequently used sites such as Facebook, Twitter, Amazon which makes up about 4 to 6 percent of internet usage. The remaining 94 or 96 percent is the Deep web and the Dark Net.



DEEP WEB

A network where data is stored in inaccessible databases. It includes all web pages, websites, networks, and online communities that are intentionally and/or unintentionally hidden that cannot be accessed using Google or other regular search engines. The deep web is used for activities such as hacking and piracy.

DARK WEB

An encrypted network that is available to a selective group not accessible by all which is accessible via authorization, specific software, and configurations. This is a marketplace for illegal goods such as drugs, firearms, and stolen credit cards numbers. The dark web is also used for human trafficking, exchanges of child pornography due to anonymity.

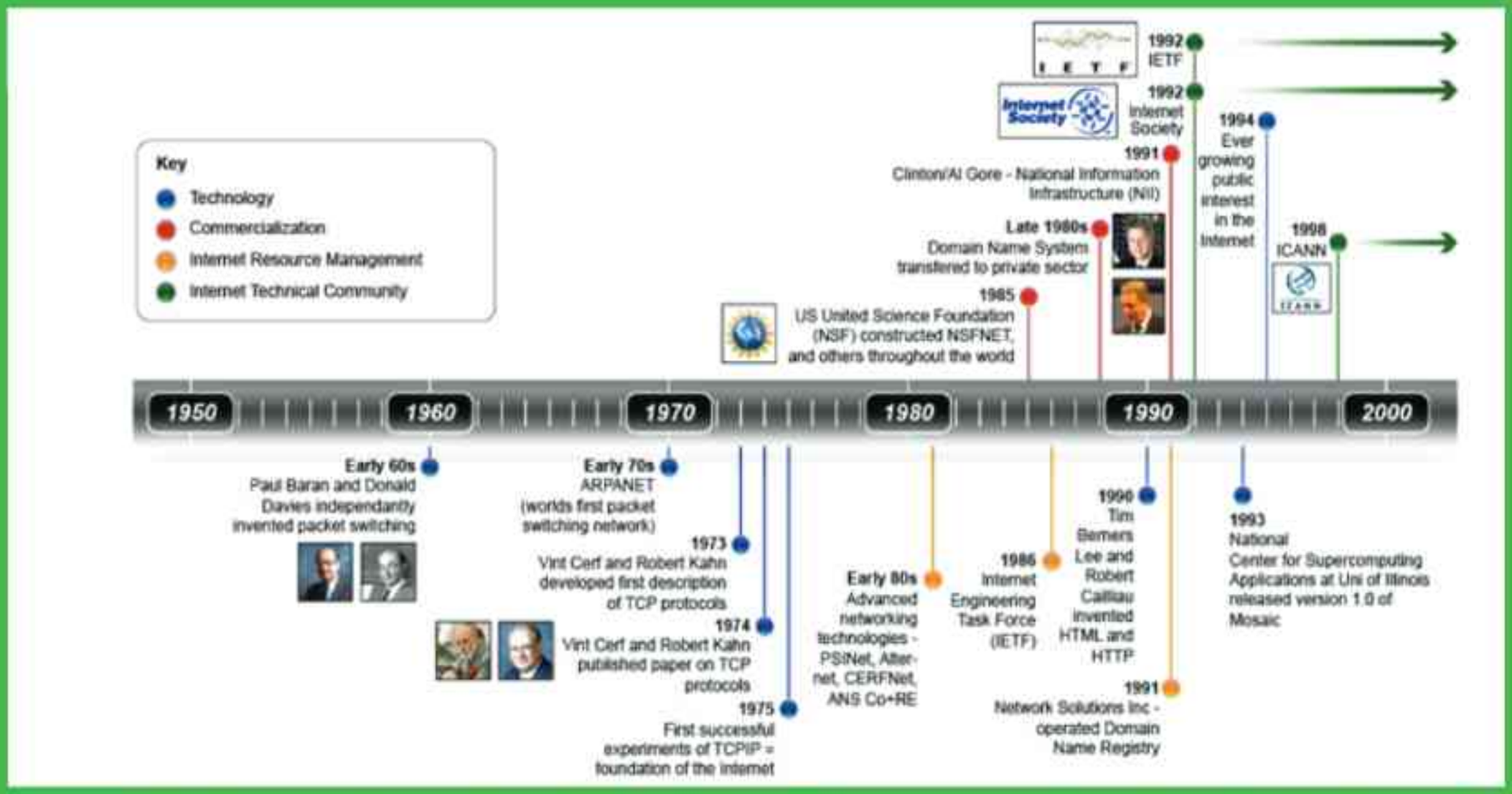
Administration Of The Cyberspace

The internet and world wide web do not respect territorial boundaries, the role of the national laws and mechanisms is limited in the management of the cyberspace. The servers of most internet service providers are in the United States and Western Europe which is beyond Indian law or any other national law. International law provides for some mechanisms for negotiations on varied aspects of cyberspace management and security. One example is the global consensus of unacceptable child sexual abuse material put online leading governments to cooperate to bring down the pages.

Digital technologies allow users to go beyond national and geographic boundaries where the government could block internet service providers. The government can also place restrictions on internet service providers with regards to any content deemed illegal or offensive.



The idea of a network of computers was thought of in the early 1960s. It was tried in different ways, and finally ARPANET was created. With time, many more changes were made and finally the internet became what we see it as today.



Source: Presentation by Dr Govind Former Senior Director, MeitY, and Ex CEO, National Internet Exchange of India and Advisor, Cyber Peace Foundation

1.4 BARRIERS TO DIGITAL ACCESS

Over the past few years digital access has become easier with devices becoming cheaper and more widely available. A range of smartphones from expensive to inexpensive are available with competitive packages offered by internet service providers.

Some attributes that define the people who are more likely to have digital access include:

* Working knowledge of English as most of the applications are presented in English.

* The knowledge of how to use a computer and related technologies.

* Easy access to digital devices and the internet.

* Ownership of the internet connected digital devices this enables the individual to receive and send information quickly compared to those who are not good at using technology.

Accessibility is uniform in that both urban and rural areas use the internet to gain information. However, socio-cultural barriers have restricted access to some important groups in society to digital technologies. This is often due to biased perception of women and girls not needing internet or for their safety they are restricted. Equal opportunities for all ages and gender needs to be established.



https://www.youtube.com/watch?v=JoxHL6EvPd8

ACTIVITY 1

THE FOLLOWING WORDS HAVE TO BE ENCRYPTED USING DIFFERENT ALGORITHMS.

For example, in the -2 series, every letter in the word gets replaced by the letter preceding two places in the alphabet. So 'apple' will become "ynnjc", "tree"will become "rpcc" and so on. In the +1 series, every letter in the word is replaced by the next letter in the alphabet. So "cat" becomes, "dbu", "sit" becomes "tju". Using similar algorithms, find the encrypted terms.

1. Deepweb (use -2 series)

- ○ Bccmucz
- ○ Accnvcz
- ○ Bccnucz
- ○ Accmvcz

2. Darknet (use 1st to last switch)

- ○ Tenkrad
- ○ Dkarent
- ○ Tendark
- ○ Tenkard

3. Bits (use +5 series)

- ○ FNYX
- ○ GNYX
- ○ FMXY
- ○ GMYX

4. Bytes (use -1,+1 series)

- ○ Zasfr
- ○ Bxtim
- ○ Czsfr
- ○ Azsfr

5. Analog (Replacing vowels with vowels and -1 for consonant)

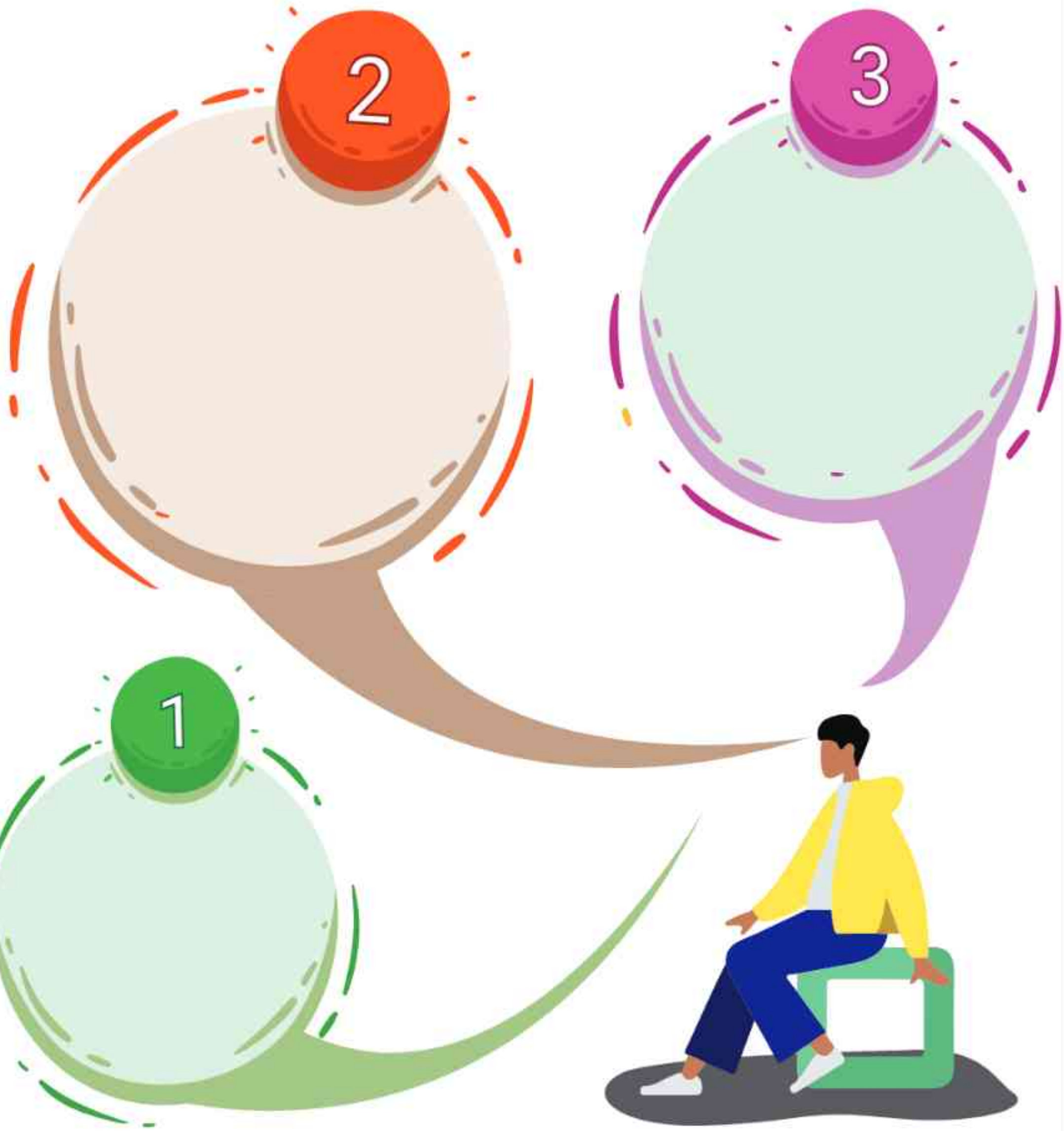
- ○ Emikuf
- ○ Arediq
- ○ Epunah
- ○ Emikof



ACTIVITY 2

EVERY INDIAN SHOULD HAVE DIGITAL ACCESS.

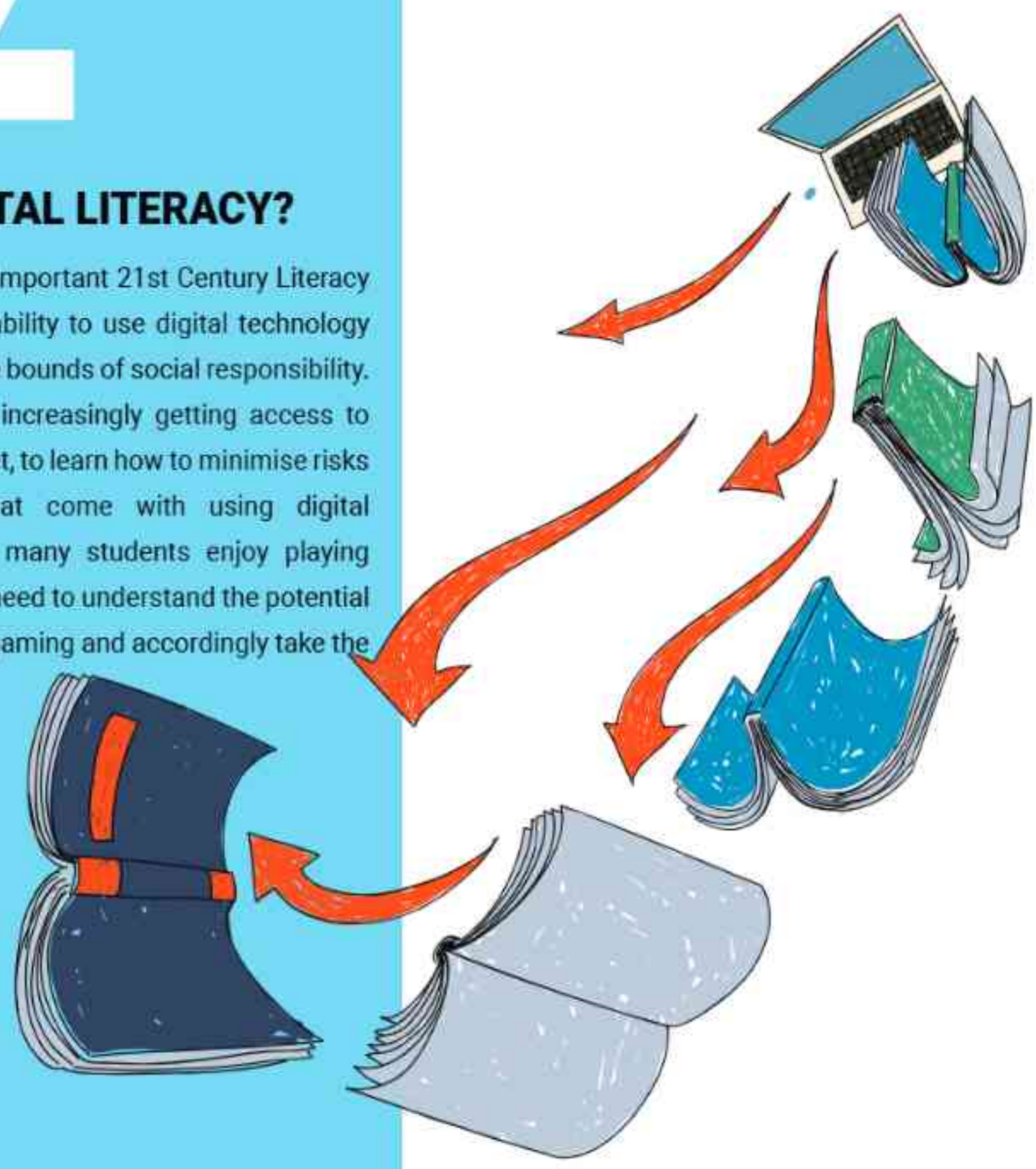
Do you agree with this statement? Provide at least three reasons in support of your answer.



02 DIGITAL LITERACY

2.1 WHAT IS DIGITAL LITERACY?

Digital Literacy is one of the important 21st Century Literacy Skills. Digital literacy is the ability to use digital technology safely while staying within the bounds of social responsibility. It allows students, who are increasingly getting access to digital devices and the internet, to learn how to minimise risks and maximise benefits that come with using digital technologies. For instance: many students enjoy playing online games, however, they need to understand the potential risks associated with online gaming and accordingly take the necessary



precautions. One such precaution includes installing a good antivirus software in order to protect personal information that is stored on your digital devices. Therefore, in order to become a digitally literate individual it is important to understand the different components within digital literacy.



2.2 EIGHT COMPONENTS OF DIGITAL LITERACY

1. Functional skills .
2. Creativity.
3. Critical thinking and evaluation.
4. Cultural and social understanding.
5. Collaboration.
6. Ability to find and select information .
7. Effective communication.
8. E-safety.



Functional Skills

Functional skills include the three Rs : reading, writing and arithmetic. In order to be a digitally literate individual, any student must know how to complete basic internet searches, work on spreadsheets etc. This allows you to access and use the several technologies present in devices, creatively and critically. This not only provides students with a new approach to their learning content but also develops their professional skills. Other functional skills also include online banking, for instance, many students use apps such a **Zomato, Amazon, Swiggy** and so on, wherein they use online payment methods. Everyone must know the safe way of sharing financial and personal information so that the risks of financial frauds, privacy breach, identity theft, unauthorised access and siphoning of money are minimised.



Creativity

Digital technologies facilitate self-expression, creativity and learning by enabling users to use different tools present. For instance: many young adults use social media platforms such as Youtube, Instagram, Tik Tok etc. To create content and share it with their friends and other audiences. This has become a new form of self-expression, wherein, individuals create an 'online persona'. However, in many cases this can lead to negative consequences as many social media personalities tend to overshare information about their personal lives, which may be used against them. Thus, they must learn to review the content they share online and should only provide information that is essential and absolutely necessary.

Critical Thinking And Evaluation

Critical thinking is essential to being digitally literate as you learn not to take information available on the internet at its face value. It is important to pause and reflect when surfing online as careless decisions online could lead to miscommunication or exposure to cybercrime.





IDENTIFYING FAKE NEWS

Cultural And Social Understanding

Children and young people are actively using digital media to participate in social and cultural life outside school. Making and sharing media has become an important part of how children communicate with each other these days. Children have to know how to negotiate information in text, visual, audio and so on and how to represent meaning effectively and creatively through these media. Children create and edit their own cartoons, videos, animations, music or other media and share these with friends. Many children may be sharing videos, YouTube, jokes, photos etc with their friends with the aim of having fun or communicating with them. Digital literacy will help to expand and extend your creative use of technology actively in your social and cultural interactions.

Collaboration

Collaboration is working among and across personal and global networks to achieve common goals. Due to the interconnected world, the effects of what is happening in one place can have repercussions in other places, what is affecting a few can affect very many.



Ability To Find And Select Information

Online browsing has made research much easier but in many ways more challenging. Now one has easier access to virtually endless information. The challenge is to check the veracity of the sources as well as the information.

01 — Is the author listed on the information/news?

If yes, they are claiming personal responsibility for the information that is being conveyed. If the information is inaccurate, their reputation and probably career could suffer. Has the author mentioned the resources used? If yes, this can help verify the information.

02 — A date shows if the information is current.

Information changes very fast, thanks to the Internet and to verify if it is still valid, a date is necessary. The information may not be relevant or credible if there is no date at all.

03 — Is the domain credible?

The domain names say a lot about websites, .com, .edu, and .gov are among the most credible domain endings for websites. Other variations are much less credible. So check the URL name. If any of those three options end a URL, it indicates the website's credibility.

04 — Is the website designed properly?

Web design is surprisingly important in verifying a website's credibility. If someone didn't put work into their website to make it look good, you can't trust that they've put the necessary effort into verifying their information.

05 — Are the spelling and grammar in the writing correct?

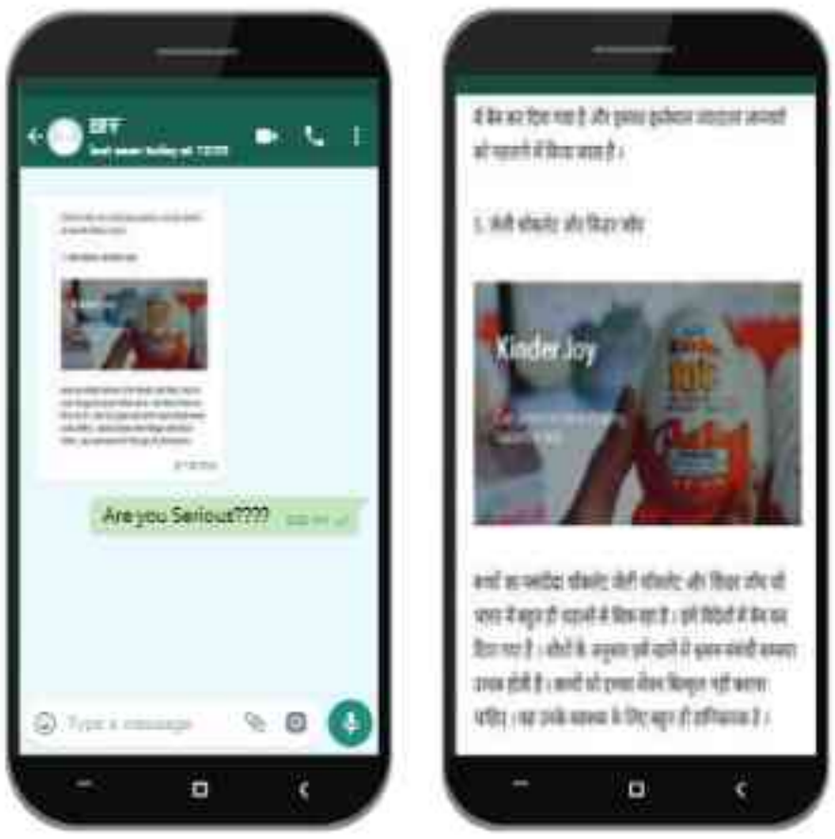
The logic is simple - it reflects how seriously the production and dissemination of information is taken. If there was no attempt to check the grammar and spelling, probably the accuracy of the information was not checked carefully.

06 — Credibility of information.

Everything on the internet or on a social network should not be taken at face value. A lot of motivated or misleading information and fake news is circulated through networks. An unbiased judgement based on critical thinking can help determine if the information is trustworthy. The recipient of information needs to decide on the veracity of the message, if need be cross-checking it from multiple sources.

The following message was circulated through WhatsApp in India in 2018. It seemed credible due to its style of presentation and language. But careful scrutiny and investigations revealed that it was false. The United States has banned the import of Kinder Joy, due to their import laws banning all commodities containing anything inedible inside, in this case the toy packed in Kinder Joy.

However, this news was presented in a slightly modified manner, and the messages implored readers to ban the chocolate as it was claimed to be harmful to health.



Online resources for digital education

Countless resources on the Internet provide information about digital technologies. Some are free while others seek payment for access to the full range of information materials. For example:

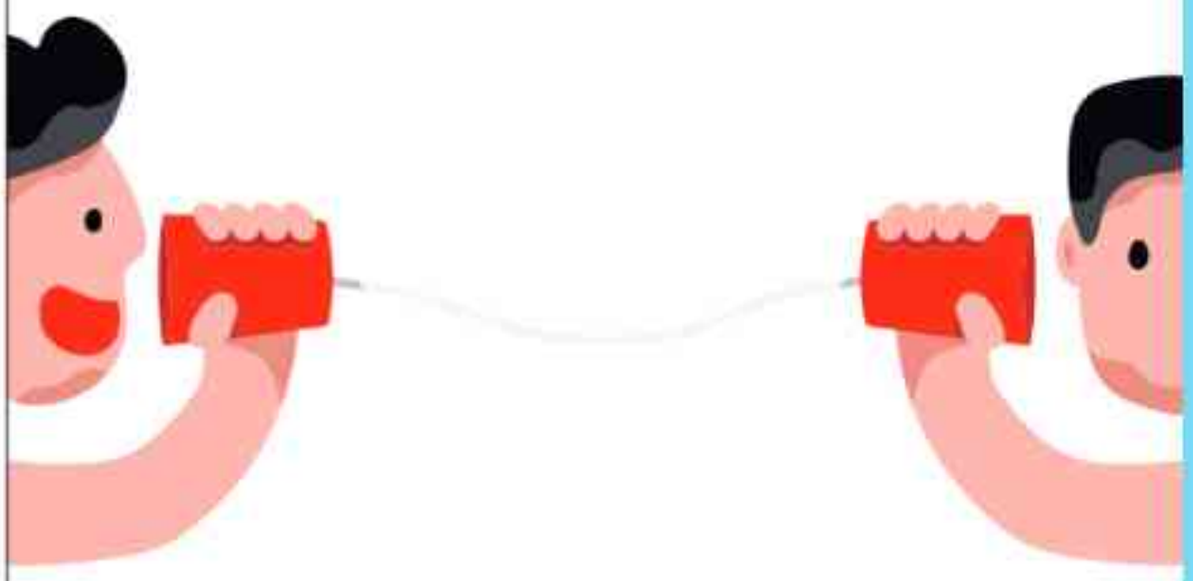
E-Pathshala, initiated by the Ministry of Human Resource Development (MHRD) and the National Council of Educational Research and Training (NCERT), hosts resources for teachers, students, parents, researchers and educators that is available on the Web, Android, IOS and Windows platforms. A wide variety of print and non-print materials, including textbooks, audio, video and periodicals can be accessed online or downloaded for offline use at **https://en.unesco.org/covid19/educationresponse/solutions**

Khan Academy makes available a range of online tools and short video lessons on its YouTube™ channel and website www.khanacademy.org, which students can use to understand various lessons and concepts easily.

Various open source resources, video lectures on YouTube™, skillshare and GitHub are available to enhance technological skills, including software development and coding. Your teachers can recommend other useful websites and portals. And you can also do your own online research.



Effective Communication



Digital technologies now facilitate immediate communication which may be one to one, one to many, or among many. This can be through voice calls, video calls, instant messaging platforms, SMSes, etc. To be digitally literate, students must understand how to engage in this form of communication safely and responsibly.



https://www.youtube.com/watch?v=fcHtksYEt-Y

E-safety

Put simply e-safety refers to staying safe online, and as internet-accessible devices are given to people of younger ages, it's important that we're able to protect them from harmful content and services. This includes: cyber-bullying, pornography, online exploitation, cyber crimes etc.



https://www.youtube.com/watch?v=bXYi-b6tiV8&t=79s



https://www.youtube.com/watch?v=-nU07_041t4&t=5s



ACTIVITY 1

State whether the following statements are true or false

a) The domain name of any website does not, in any way, indicate the website's credibility.

b) When reading offline, the resources may take several seconds to open as the entire file is encrypted. However, once that process is complete, pages open rapidly.

c) Critical thinking is one of the components of digital literacy that involves the process of evaluating information, questioning it, and determining if it's worthwhile or not.

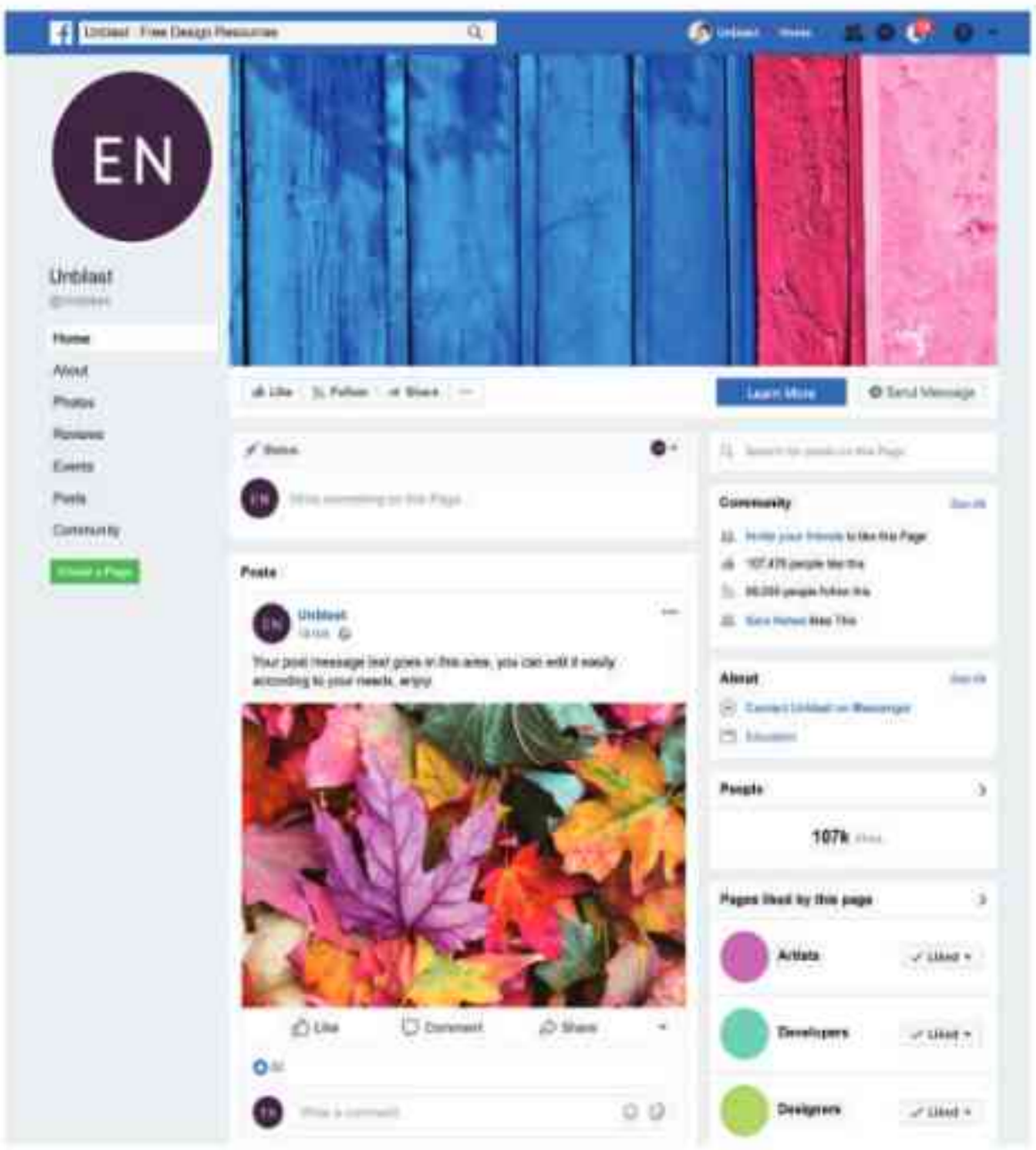
d) E- Pathshala, an initiative of Ministry of Electronics and Telecommunication (MeitY) and the National Council of Educational Research and Training (NCERT), hosts resources for teachers, students, parents, researchers and educators.

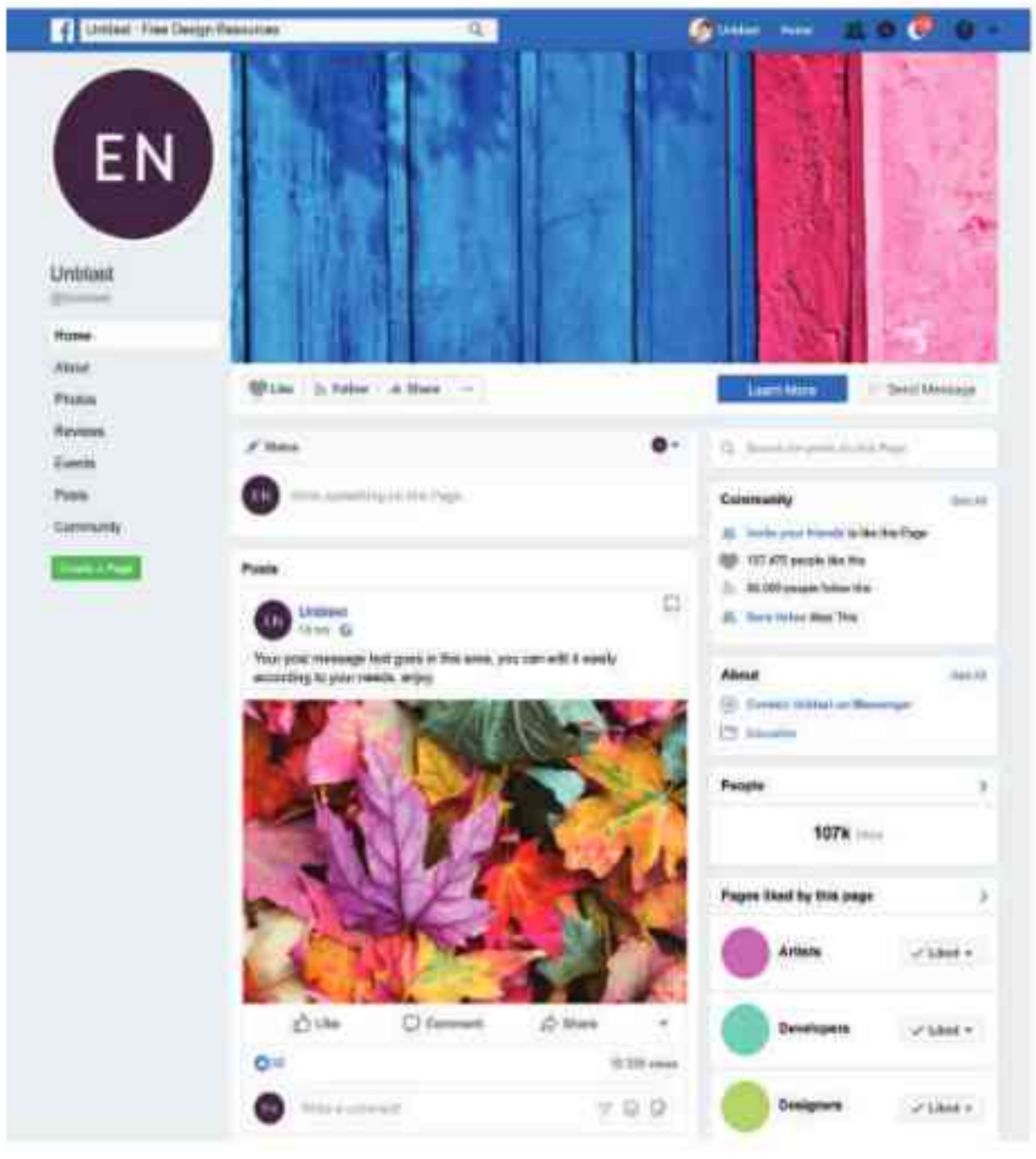
e) Critical thinking not only improves our functional skills but also facilitates learning and provides new avenues for professional advancement.

f) Digital literacy involves the ability to read, understand and interpret digital processes whereas, digital communication is the ability to communicate, connect and interact with others.

ACTIVITY 2

Is the information given below reliable or not?
Give reasons to support your answer.





03

DIGITAL COMMUNICATION

3.1 WHAT IS DIGITAL COMMUNICATION

Digital communication is the ability to read, understand and interpret digital processes to connect and interact with others. It can help stimulate social relations in cyberspace. The users are able to stay in touch with friends or make new friends. Those who are not good with social relations can use it to compensate and build new positive relationships.

Mobile phones are the primary source of access to the internet in India. The world's cheapest mobile data packs have been offered in India as mobile companies in a competitive telecom market have tried to offer the best and cheapest plans. A study conducted across 230 countries over a period of one month found that Indians were paying an average of Rs 18 for a gigabyte of data compared to the global average of Rs 600. Not surprisingly, the number of internet users in India was more than half a billion with the usage being equal for both rural and urban areas.



Box 3.1: Circuitry of digital communication

In a simple one-way communication, there is a sender who uses a medium such as a phone to send a message to a receiver. Verbal communication involves someone speaking and someone listening. Interpersonal communication occurs when the sender and receiver exchange their roles, and speak and listen to each other through a process that facilitates understanding, agreement or disagreement. Visual communication involves someone showing a visual product (e.g., a picture, video, animation) and someone watching.

Digital communication in the virtual world can allow for interaction between more than one person such as an email can be copied to many people. However, it requires a balance between the real and the virtual world.

Real versus virtual lives

Real lives	Online lives
Offline activities	Online activities
Direct socialising	Social networking
Face-to-face communication	Text messaging
Personal Interactions	Internet connections
Life in local community	Life in worldwide web
Relatively private existence	Greater public interactions
More engagement demands	More escape opportunities
Limited information	Unlimited information
Careful communication	Less inhibited communication
Greater responsibility for personal actions	Evasion of responsibility possible with perceived anonymity
History remembered	History recorded (digital footprints)
Parents feel more in control	Parents feel less in control

Everyone needs to be conscious of the differences between real and virtual life and use technology in a way that it does not become a substitute for real life communication but remains a smart additional channel which is not allowed to compromise basic good interpersonal communication skills essential for success in all aspects of our life.

In-the-moment communication through instant messaging, texting, and posting comments online is common. It does not allow enough time to reflect, react and respond on the basis of informed understanding of conversations that are getting rude or mean. But learning to exit such conversations is essential. You may have to sign off instant messaging, not respond to a rude text, or stop yourself from posting a comment on Facebook or Instagram.

3.2 OPPORTUNITIES AND RISKS

Online activities provide an opportunity for expressing our opinions, testing attitudes, and exploring identity and social relationships. But many of us are tempted to take risks, often under the misperception that we are anonymous online. Sometimes we show weak control over the time spent online activities, and setting and focusing on priorities. Outdoor activities are essential for good health and can also help to prevent excessive use of digital devices and addiction to online activities, such as gaming.

The expansion of the internet has led to a shift from face-to-face communication to digital communication. Even people in close proximity can be found exchanging messages on their mobile phones.



Social media has provided children with a platform to express themselves to a limited audience - typically those who are similar and have comparable values, beliefs and attitudes. As a result, it has made communicating with different people more difficult.

There is a tendency to use internet as a substitute for real relationships and the content we encounter online can influence us by creating an artificial digital environment. Moderate use of the internet and a balance between offline and online lives is crucial for adding value to our life and work while minimising risks and harm. Being smart online means being aware of the potential threats, opportunities and risks that might occur without losing sight of the things that are most important in our lives.

Responsible Sharing



Take responsibility for your online communication.



Forward information or posts only after verifying the source and contents.



Avoid sharing posts that are offensive or obscene.



Personal information that you share can be used against you. Review the content that you wish to share online and only provide information that is essential and absolutely necessary.



Use trusted sources for downloading online. Downloading songs and movies from untrusted sources may be illegal and you should not be sharing these with your friends. Use trusted websites or platforms, like Google Play Store, Apple App Store etc.

Personal Responsibility For Information Posted Online And Sent Via Text

"Posting Photographs"

Often family, friends, acquaintances and strangers post photographs on social networking sites. Usually they do not seek consent of the person whose photograph they post. While their intention may not be bad, the photograph can be misused by a wide variety of other people. It is a good idea to convey your concerns if you do not want your photographs posted.



Many parents overshare pictures of their children online and in the process undermine their right to privacy, cause embarrassment, hurt and bullying, and damage online reputation.

Sharenting reveals aspects of children's life on social media without their consent. They may be too young to fully understand but it is important to consider the consequences from their perspective. Posting of a picture of a child with a funny caption, relating to their hair or facial expression, could upset them when they are older or make them a butt of bullying by others. Every post contributes to a record of photos, shared links and comments. This record is hard to delete and can shape the child's online reputation.

4k 200

Sharenting and its risks

"Stranger Danger"

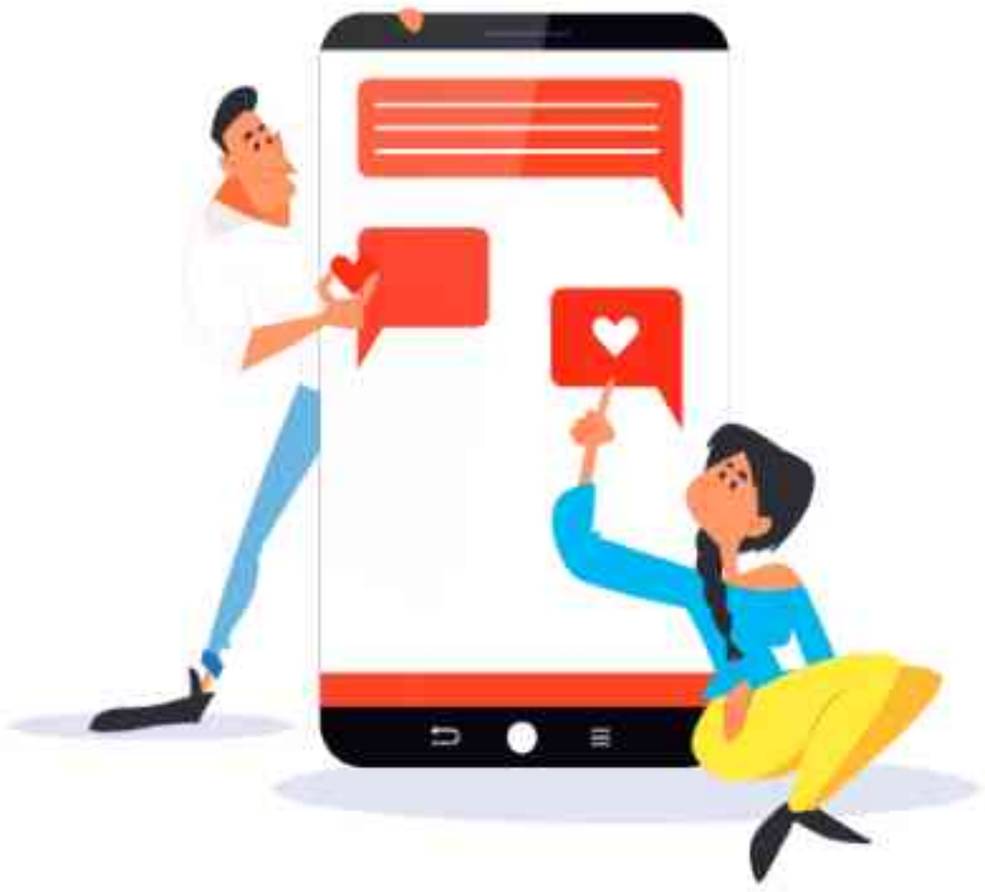
As in real life, there are strangers, acquaintances and friends online. How one communicates, how much and what kind of information is shared depends on the equation and level of trust people have in one another.

It is important to choose online friends wisely. Be wary of new online friends. Do not trust them easily because who knows who they are. There are many cases of people faking identities with not so good intentions. They may be people known to you, who wish to dig out more information out of you. They may be strangers, who wish to gain and then betray your trust.



"Grooming"

Sometimes strangers, or even people who are known, build an emotional connection with children and young people online or face-to-face to gain their trust for the purposes of sexual abuse or exploitation. Many children and young people begin to feel that a special friendship or relationship is developing and do not understand that they are being groomed. "Grooming" is subtle but has serious consequences.



Recognize Ways That People Online May Seek To Persuade You.

a) Bribing: This can range from offering money and gifts. The gifts may even be in the form of points or lives and in-game rewards in an online game.

b) Flattery: Constant attention and praise can be a way of winning the affection of the targeted child.

c) Sexualized games and intimacy building: Gradual introduction of subtly sexual allusions in conversation or during play are used to test the child's vulnerability. If the child positively responds to his overtures, he will attempt to build further intimacy with the child.

d) Desensitization: They try to desensitize the child to sexual acts by showing the child, pornography and child sexual abuse imagery. Constant exposure to explicit content may 'normalize' sexual behavior for the child and 'desensitize' her/him.

e) Threats and blackmail: They employ forceful coercion to gain access to the child.

f) Scattergun approach: When they do not know what the child will respond to, they may try all of the above in an effort to win the child's attention and interest.

Inform and discuss with friends, family members, teachers or anyone you trust any annoying or uncomfortable occurrence or activity such as extra friendly behaviour, cyber stalking, bullying and strange behavior online.

Viewing Inappropriate Content

While accessing the internet you may come across content that is not suitable for your age, the content may include images or information adult in nature, maybe sexually explicit or very violent. Accessing inappropriate content is possible through websites, gaming apps or by clicking links which may be intentional or unintentional. One way to avoid this is to use apps and games that are suitable for your age.



If you are going through something similar, do not hesitate to report such profiles.

Gaming

Games can offer children a way to escape from the real world and immerse themselves in a virtual world. Increasingly, children play games on mobile phones, consoles, laptops, computers, portable gaming devices and social media. While playing you could interact with other gamers through a microphone or a webcam. Cybercriminals can find a way to victimise children through befriending them online, cyberbullying or sharing inappropriate content. Children should be made aware of the risks and how to handle certain situations.

Potential Risks Associated With Online Gaming

a) Some games let children play and chat with anyone in the world. There are many aggressive players online who may bully you.

Some players play simply to bully or harass others. They may use inappropriate language or cheat others. It is important for you to be careful.

b) Some young people through online games are abusing the fear around the challenge to encourage others to self-harm and carry out various dares and post the results online under the guise of some game challenge. Do not give in to such provocation and/or challenge. Stop playing such games and inform your parents/ elders.

c) Many adults and cyber criminals pretend to be children while playing online games. They may try to befriend you by giving tips about the games, sharing points with you and trying to win your trust. They may use this opportunity to get your personal information or influencing you for a one-to-one meeting.

d) Some games may have content which might upset you. This could include violence, horror, or sex or induce you to self-harm. Do not play these games and talk to an adult if you are upset.

e) Online games are sedentary in nature and children can be involved for long periods without moving around. It is good advice to take breaks every hour or alternate online games with outdoor activities.

f) Be aware of when you feel like you might be getting addicted to online gaming. Check if your online games, stop you from seeing your friends or family.

i) Take the place of doing homework
ii) Make it hard to stop thinking about playing
iii) Make you unable to stop playing, even when you need to sleep.

If you feel this is happening, it's a good idea to get support. Talking to someone you trust, preferably an adult or a professional counsellor. Either they may be able to help or help you find someone who can help.

Know the risks, exercise good judgment and seek advice. What you do online has the potential to affect everyone – at home, at school and around the world. Practicing responsible online habits benefits the digital community.

3.3 SAFETY AND SECURITY DURING ONLINE GAMING

GOOD PRACTICES: HOW YOU CAN PROTECT YOURSELF WHILE PLAYING GAMES ONLINE

Prudent Selection Of Games To Play

a) Check the age classification of the games you want to play. Stick to the ones that have been indicated for your age group.

b) Never install games downloaded from free online gaming websites that are not reputed. Never download games by clicking on links received on mail or text message or through a pop up.

Protect Personal Information

a) Always install a good antivirus software on your computer, smartphone or other handheld devices. Regularly update the antivirus and other applications.

b) Do not share personal information like name, date of birth, address or phone numbers while playing online games.

c) Never share your passwords with anyone. You should use a complex password for your online gaming account and other online accounts. It is a good practice to change your password at regular intervals.

d) Never use voice chat or webcam while playing online games. This may share your identity with other players and attract cyber bullies and other cyber criminals.

e) Never share your or your parent's credit card/debit card details with anyone when you are playing online games. They may ask credit or debit card details. Never share such details with anyone.

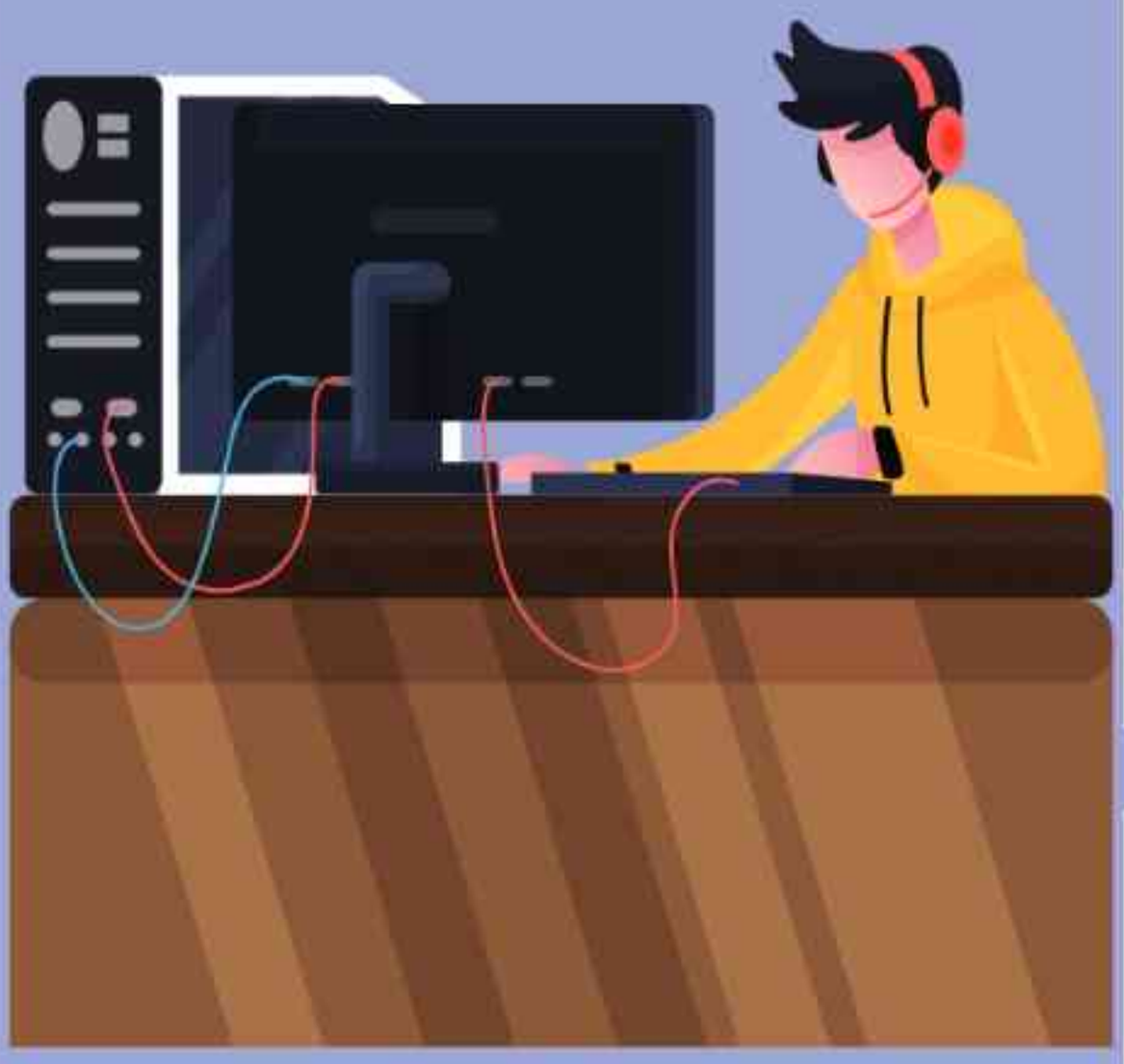


Know How To Respond To Online Challenges

a) Know the tools that are available to deal with aggressive or inappropriate conduct online. Learn how to block, mute, delete and report on the games and consoles being used.

b) If you face any challenge in online gaming world, immediately inform your parents or elders so that they can support and guide you.

c) Never meet in person with someone from your online gaming world. In real life they may be very different. Cyber criminals may befriend you and try meeting you or getting your personal information. They may have wrong intentions.

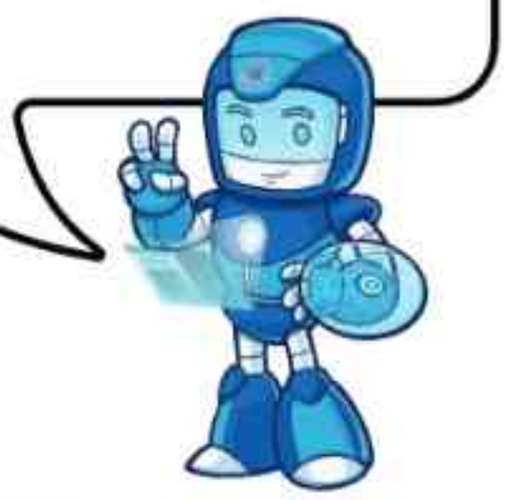


Limits In Friendships

Set limits to your online friendships as well as online communication with real life friends. There has to be a limit to what you share or exchange in terms of written words, photographs or videos. Remember, once online, you may not be able to control who will actually see it, prevent breach of trust and misuse and potential risk and harm to your person and reputation.

A class 8th girl's Instagram account was hacked by one of her classmates. He used her account to send obscene messages and videos to her friends and also to all the people who were added in her account. Next day her friends didn't talk to her nicely and those who did were rude in their behaviour. The girl did not understand the situation and this kept on happening for a week. The girl was in despair and asked one of her friend as to why is everybody avoiding her. She was surprised that all this had happened. She spoke to her friends, clarified the situation and sorted the problem. The problem that still remains is that her account is still being used by someone even though most of her friends have reported that account.

Learnings: Always make sure that you use strong passwords and do not reveal them to anybody, not even your best friends. Make sure that if something like this happens, you tell it to your parents, elders, and teachers. Also in such cases report to cybercrime branch of the police.



Revenge Pornography

"An act whereby the perpetrator satisfies his anger and frustration for a broken relationship through publicising false, sexually provocative portrayal of his/her victim, by misusing the information that he may have known naturally and that he may have stored in his personal computer, or may have been conveyed to his electronic device by the victim herself, or may have been stored in the device with the consent of the victim herself; and which may essentially have been done to defame the victim."

Teenagers in the age-group of 14 to 18 years are the worst victims of revenge porn as well as the perpetrators themselves, which is a matter of concern. Some teenage students who have been in a relationship and end it find their explicit photographs circulated on social media platforms or tags her in the pictures or sends her a link. When such images go viral, students are often harassed and bullied by their peers – branded with insult and in the end, isolated. A teenager may be targeted by her jealous classmates, her ex-boyfriend or even an unknown friend on social media who

may be victimising her because she stopped communicating with him when she realised the dangers of online relationships.



Revenge pornography can lead to students dropping out of schools and preferring to stay home or change schools. This may make students go into depression or feel isolated. Students often do not report such cases to teachers or parents due to the fear of the problem becoming bigger.

While some teenagers may know the dangers of sexting, peer pressure forces them to indulge in this as due to peer pressure and not wanting to be left out of the group. Children should not succumb to peer pressure, especially to take risks of this kind which can be extremely embarrassing and damage their reputation. In extreme cases children have been driven to suicide. Do not give in to pressure. If you lose your inhibitions you also lose control. Once you have pressed the enter key you cannot retrieve your message and may make yourself vulnerable to potential harm and exploitation.

However, teenagers need to understand gender relations. Boys must learn to interact with girls on equal terms and respect them and their desires as those of human beings, not simply as objects of respect or desires. Consent must be an important part of relationships. Pictures, videos and other material shared in confidence cannot be published on social media without the permission of the person just because the other person does not want to continue in the relationship. Youngsters must learn to cope with rejection as it is a part of life but not the end of the world.



https://www.youtube.com/watch?v=0AxfdpuyHS4&t=148s

ACTIVITY 1

Classify the following statements as legitimate or illegitimate while chatting with online friends or while surfing online websites/gaming.

Statement 1 – If you disclose your age and address of your residence, you shall be getting 350 bonus point for the current session of the game.

Statement 2 – I like the way, this conversation has been continuing, I wonder what it would be like to catch up with you in real life.

Statement 3 – I have all the details of all our conversation in this chat box, if you do not send me pictures that I ask you for, I would make these conversations public, without hiding our identity.

Statement 4 – I am sending you some video attachments, and after watching the same, you have to send me similar videos.

Statement 5 - Hey tell me the sizes of your chest and waist, so that accordingly, we can design a costume for you, before entering into the next level of this gaming session.

ACTIVITY 2

Substitute one word for the following statements

A way of communication where a sender who sends a message through a medium to a receiver is known as _____ **A**

_____ involves an act of giving constant attention and praise in order to win the affection of the targeted child. **B**

_____ offers young people a sense of escape from the reality of the world and, at times, it can make them feel that they are a part of a community. **C**

An act of posting, or distributing, or sharing of any sexually explicit images or videos of the victim on the social media websites to take revenge against a broken relationship is known as _____ **D**

ACTIVITY 3

What steps should be taken while playing an online game, which involve interactions with strangers?



04 DIGITAL COMMERCE

4.1 WHAT IS DIGITAL COMMERCE?

Digital commerce is about the users undertaking legitimate and legal exchanges using digital technologies. The new digital economy has improved the choices of goods and services to the consumers. They can choose what they want from a wide array of products offered by an ever expanding market of online vendors. The virtual market place is assisted by a growing network of financial and other service providers. Websites provide outlets for sales of goods and services. A growing number of brands are available online to consumers directly through their own platforms or through aggregators.



a) Buy and sell (e.g., Amazon, Flipkart, eBay, Facebook "marketplace",...).
b) Book travel (e.g., IRCTC, MakemyTrip, RedBus.in, booking.com).
c) Book hotels (e.g., Trivago).
d) Order food (e.g., Zomato, Swiggy).
e) Sell used products (e.g. Olx, Quikr, ebay).
f) Make payments (Paytm, Google Pay, Bhim, UPI, credit and debit cards, and netbanking).
g) Advertise goods and services.
h) Pay taxes (e-payment portals).

4.2 OPPORTUNITIES AND RISKS

E-commerce has both risks and an abundance of opportunities. One risk that individuals encounter is e-payment methods. An e-payment system is a way of making transactions or paying for goods and services through an electronic medium, without the use of checks or cash. It's also called an electronic payment system or online payment system. The electronic payment system has grown increasingly over the last decades due to the growing spread of internet-based banking and shopping. As these increase, improve, and provide ever more secure online payment transactions the percentage of check and cash transactions will decrease. But you are also susceptible to financial frauds, involving privacy breach, identity theft, unauthorised access and siphoning of money.

Individuals also face a form of fraud called phishing or vishing. Malvertising and piracy are also common risks of engaging in digital commerce.



What Is Phishing Or Vishing?

A target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords. For instance: A student's grandfather recently told her about a credit card scam that happened to many of the residents in the old-age home where he lived. He told her that they were called by an anonymous number posing to be a bank manager and asked for their credit card details including the pin number. As a result, the scammers wiped out all the cash from their accounts. They lodged a



complaint regarding the situation which led to the scammers being caught but most of them have not got their money back.

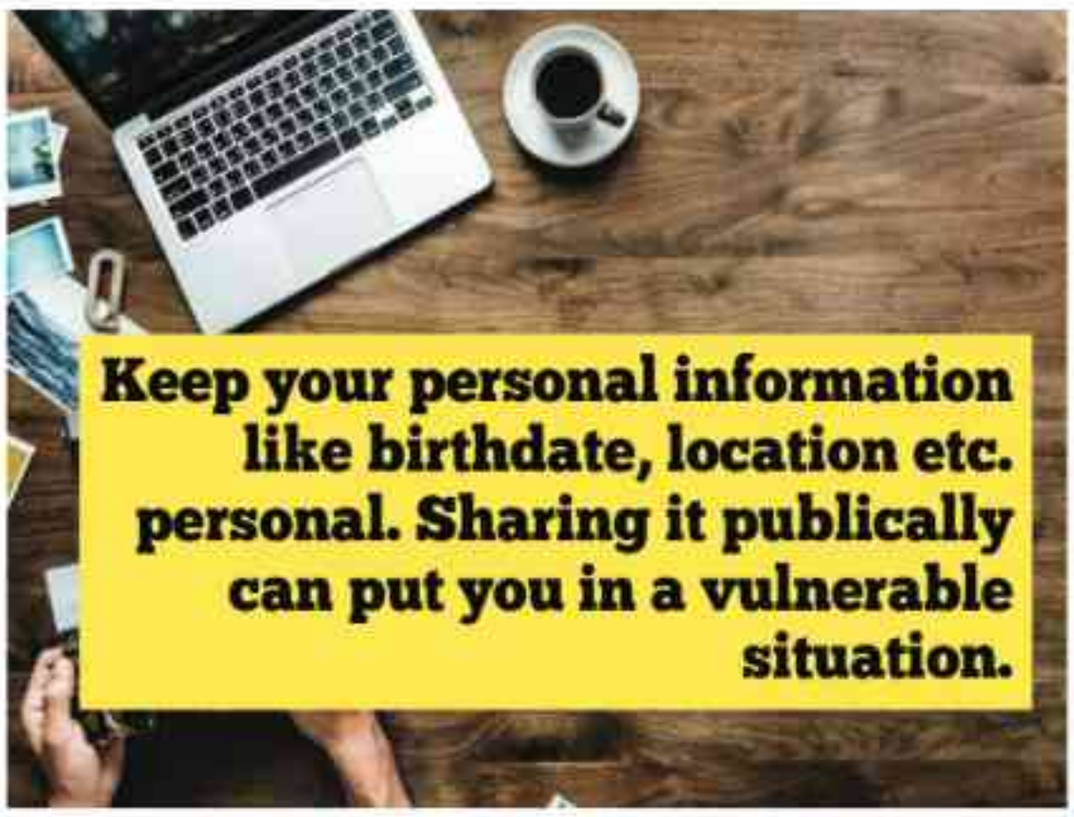
What Is Malvertising?

Malvertising It is the process of using advertisements to infect your devices and systems with malware. These ads look legitimate and trustworthy, by one simple click will cause your phones and computers to be compromised.

What Is Piracy?

Production and consumption of pirated music, software, games and videos is common but illegal.

4.3.1 How To Avoid These Risks?



Safety Measures:

a) Install a robust anti-malware and antivirus solution .

b) Be extra careful while visiting websites that ask for personal and financial information .

c) Never click on suspicious email messages, especially those offering loans and too good to be true deals.

d) Shop only at websites you trust. Check the security features of new websites and the authenticity and customer reviews of the business.

e) Keep the receipt, order confirmation number, and postal tracking number safe.

f) Report if you do not receive merchandise of the promised quality.

g) Secure your digital devices linked with bank accounts with strong passwords and good antivirus software. Choose unique, non-guessable and meaningless passwords.

h) Computers in cyber cafes may not have updated antivirus or may be infected with malware, which may compromise your bank details and other sensitive information such as card number, expiry date, CVV, etc. Thus, avoid making online financial transactions using a public Wi-Fi or a computer in a cyber cafe.

i) Disconnect the phone after receiving any call from anyone claiming to be a service provider, who seeks sensitive information to avoid deactivation of your number or making a just too generous offer. Immediately call customer care to check if such a call is genuine.



Do connect to secure public network whenever possible. In the event that you are unable to connect to a secure network, try to login only if it asks for registration.









4.3.2 Cautious Browsing

If the website looks strange, the address in the address bar looks off, or the site starts asking for information that it normally doesn't, check to ensure there is a lock icon in the address bar, denoting a secure website, and click on the lock to ensure that the website has a trusted, up-to-date certificate.

4.3.3 Online Purchases And Sales

Download only from verified and secure sources like PlayStore and AppStore. Downloading from other sources may lead to your devices being infected by malware.

Resist the temptation to open emails and attachments from unknown sources, especially those offering special deals or surprises. For example: legitimate websites will send emails that are grammatically incorrect.

Some offers may be too good to be true. Beware of such offers as they may be fraudulent.

Compare the prices of the product at different sites to avoid being overcharged. Make payment only after you have verified the buyer and the products.

Hazards Of Providing Sensitive Information Online (Credit/debit Card Info, Sharing Otps, Account Numbers, Etc)

Some of you may be using banking services such as debit card, credit card, net banking, etc. at this stage but as you grow up many more may start using these services. As a smart citizen you must understand how online transaction frauds can happen so that you can be safe yourself, teach others in your family and friend circle.

Cyber Criminals Cheat People Online In Many Ways

They may send an email to a bank account or credit card holder from a fake account, which appears to be from their bank or credit card service provider. The unsuspecting user who clicks on the link provided in the email is taken to a page where he or she is asked to share details of the bank account or card, card verification value and expiry date. Once such sensitive information is shared, their bank or credit card account is seriously compromised.

Posing as a bank employee, they may try to obtain credit card or bank details such as account number, personal identification number (PIN), CVV, expiry date and date of birth. Once such details have been provided, the account is seriously compromised. As mobile numbers are usually linked with bank accounts, posing as an employee of the mobile service provider they may call and inform the user that his or her mobile number will be disconnected if they do not update their Subscriber Identification Module (SIM).

They attempt to make the user to click on a link or send an SMS to a number shared by them. They claim that the link and number will connect the user with the service provider but are actually trying to establish a connection with a duplicate SIM obtained fraudulently from service provider. If the unsuspecting user falls in the trap, they use the duplicate SIM to transact online using the victim's mobile number and banking app.



The victims of such financial frauds experience serious problems. They end up being saddled with debts for monetary transactions they have not done. In order to avoid liability for debt repayment, they have to provide proof that they have indeed been duped. The process can be difficult and time-consuming.

Check The Website URL. Https Encrypts Your Data In The Website And Protects It From Any Kind Of Tampering. Do Not Share Your Confidential Information Such As Online Account Password, Card Number, CVV, Expiry Date, Pin And OTP On The Website Which Does Not Start With https.







WATCH

https://www.youtube.com/watch?v=0sAFjBFTf3c&t=29s

Scams Using Ids Of Army Officials



Many scams are being operated using stolen/fake identities of army officials.

WATCH

https://www.youtube.com/watch?v=UHzgYY7tgkk

WATCH

https://www.youtube.com/watch?v=6cXX6YBwrHQ

WATCH

https://www.youtube.com/watch?v=gQtY4pua5eM&t=6s

WATCH

https://www.youtube.com/watch?v=4dsFKIY-tYw&feature=youtu.be

WATCH

https://www.youtube.com/watch?v=TmgqNe_KjBg

WATCH

https://www.youtube.com/watch?v=tO22q6ejk8w&t=8s

ACTIVITY 1

Match the following terms with their definitions

Terms		Definition
Phishing		A — Production and consumption of pirated music, software, games and video.
Vishing		B — A specific kind of software that blocks the user from accessing their devices/systems until a ransom is paid.
Malware		C — A phishing scam that infects multiple users at once.
Ransomware		D — An act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft.
Pharming		E — A cybercrime in which a website's traffic is manipulated and confidential information is stolen.
Piracy		F — Process of using advertisements to infect devices and systems with malware.
Malvertising		G — Software designed with the intent to disrupt, damage, or gain unauthorized access to a computer system.



05 DIGITAL ETIQUETTE

5.1 WHAT IS DIGITAL ETIQUETTE

Digital etiquette is about being aware of and behaving in an appropriate, responsible and ethical manner while using digital devices and technology. This includes shaping your digital reputation and being a responsible citizen of the communities in which you participate, from school groups, to games, to social networks.



5.2 OFFLINE ETIQUETTES ARE ALSO ONLINE ETIQUETTES

Sometimes children use digital devices and technology in the wrong context. For example:

a) Using mobile phones while talking to someone constitutes a social faux pas or even an insult to the other person.

b) Texting while carrying on a conversation with someone is very rude and shows disrespect.

c) Using mobile phones in classrooms, meetings and social gatherings. Using cell phones to text while attending a class is not appropriate.

d) Ping others late at night. There is a time for everything. Do not disturb others at night. You may also not like to be disturbed when you are trying to rest.

e) Playing audios and videos loudly in public. It is rude and inconsiderate to others.

Agree To Disagree

Make respectfully disagreeing the norm. Respect the opinions of your classmates. If you feel the need to disagree, do so respectfully and acknowledge the valid points in your classmate's argument. Acknowledge that others are entitled to have their own perspective on the issue.

Avoid Digital Drama

"Digital drama" in the form of hurtful comments, mean-spirited rumours, and embarrassing photos, is a pretty common online occurrence. Such posts spread quickly and cause immense harm to someone. Perception of anonymity may give a false sense of complacency and false bravado. Lack of sensitivity or thought can impact friendships and creates unnecessary and avoidable tension in the network and community. Just think how you would feel if the same happened to you.



Treat others online the way you wish to be treated. Before posting, ask yourself:

- Would you say that to someone's face?
- How would it make the person feel?
- Could someone take your message the wrong way?
- Will this hurt someone's reputation?
- How would you feel if someone said that to you or wrote that about you?
- Would you want your friends, parents or teachers to read this about you?



It is easier to say hurtful or disrespectful things without standing face-to-face with someone, however, it is important to remember that your classmates and teachers are real people who are affected by the words you say and write. It is essential to keep in mind the feelings and opinions of others, even if they differ from your own. If you wouldn't say it to someone's face, don't say it online either.

If you feel hurt after reading a post from a friend or a stranger, do not react with an aggressive reply. If hurtful post or message is from a friend, request him not to do it again. If you are repeatedly getting such messages/ posts, please inform your parents or elders immediately so that they can support you.

Also, please remember that as a good digital citizen you should not share mean comments or hurtful messages or embarrassing pictures/videos online. Please be careful and check if your post/comment /videos can be embarrassing for your friend or anyone else. If so, please don't post.

5.3 BEING POSITIVE ONLINE

Students are encouraged to take an active role in building positive, supportive online communities. Here are some things you can do to contribute to a positive online environment.

5.3.1 Posting Positive

As a responsible digital citizen, always review your messages and posts to be sure that they are not untruthful, negative, sarcastic or rude.

5.3.2 Being Responsible, Honest And Truthful

Misleading others is a major breach of online etiquette. This is true even if it is unintentional.

Check facts before providing information or giving advice online. Misinformation will just add to the clutter of the internet and waste people's time.

Avoid posting anything that is not true such as rumours or gossip.

So do not be naive and forward that message hoping it will bring you good luck. Many viruses are spread via chain messages and invitations. If you wish to forward information, make sure it is verified and shared with people you know.



Check The Accuracy Of Your Messages

Forwarding messages without checking their accuracy: This may contribute to the phenomenon of "fake news" and rumour mongering.

Double check messages before hitting the send key. Pause and think about your posts, comments and e-mails before you send it. Once you press the send key, there is no way to take back the messages. Sometimes a message that is meant to be funny, may not come off that way at all because the person on the other end cannot see your facial expressions or hear the tone of your voice. Read your messages again to see if they can be misunderstood. It is best to discuss sensitive or difficult issues with the person directly rather than posting something online or sending a hurtful e-mail.

5.3.3 Respecting People's Confidence

The ability to keep information shared by someone in confidence reflects a strong character. Do not reveal the information online (or off-line) if the answers to the following questions was "yes".

- Was this information supposed to be confidential?
- Will it embarrass the source of information?
- Will sharing this information compromise someone's privacy or create drama?

If the answer to these questions is "yes", do not reveal the information. That is what a good friend would do.



Always ask permission before uploading someone's pictures and posting personal details. It constitutes a violation of the privacy of the person whose pictures or personal details have been posted.

Cluttering other peoples' inboxes, which annoys most people. Tagging your friends may seem harmless but it is important to get their consent. Everyone does not see things the same way and you may strain your relationship.

5.3.4 Posting Positive

Do not post anything that you do not want to last forever. Before you say or post anything online, ask yourself, "Am I ok if this is never deleted? Once something is posted online, it is likely to be there forever. As of now, there is no delete button or eraser for the Internet.

Avoid inappropriate use of technology. Users have a responsibility to use technology appropriately without harming or inconveniencing others. Many users often use technology inappropriately without understanding the consequences.

For example, Spamming is the sending of unwanted bulk messages indiscriminately through emails, internet forums, instant messaging, social networks, mobile text messaging, fax transmission, advertisements, and other networks.



5.4 CYBERBULLYING AND CYBERSTALKING

A fine line separates bullying from teasing. Different people have a different threshold of tolerance for being able to take teasing or cyberbullying. Know and understand what cyberbullying is and never engage in that kind of behaviour.





Teasing Versus Bullying

a) Teasing typically happens among friends or kids trying to fit in with their peers.

b) When it goes back and forth equally between kids, it's usually playful. If one person asks for it to stop, the other does so.

c) For adolescent boys, teasing is a "rite of passage". Teasing can get rough, but it's not meant to hurt the other person.

d) A bully fully intends to harm his or her victim and has the power and the means to do so. This person might be more popular or physically stronger, and the victim may have a hard time defending himself.

e) Children who are seen as different or don't "fit in" are typical targets of bullying. This includes children who have a disability, are overweight, or are thought to be homosexual.

Unacceptable Use Of Technology To Bully Others

Being at the receiving end of offline or online bullying can be very distressing for anyone. Under no circumstances can such behavior be considered acceptable.

VARIOUS FORMS OF CYBERBULLYING

- Making fun of another user in internet chat rooms.
- Harassing a user over instant messaging sessions.
- Posting derogatory messages on a user's social networking pages.
- Circulating rumours about another on social networking sites.
- Publishing lewd comments about another person on personal blogs.
- Posting unflattering pictures of another user on the web.
- Sending unsolicited and unwanted email messages (also known as spamming).
- Sending threatening or provocative emails.
- Repeatedly calling another person's cell phone.



"Trolling is also a type of cyberbullying, where repeatedly harassing or intimidating comments are made.

The cyberbullies can be known people, known people hiding their identities, or strangers who use digital technologies to send nasty text messages or emails, or set up hate groups on social networking sites. The victim is often targeted constantly or periodically even when they are in the comfort of their own home. The technologies enable them to circulate messages or images very quickly and widely on the internet, which makes it very hard to combat cyberbullying. Cyberbullying takes place between two young people.

How To Deal With Cyberbullying?

Prevent cyberbullying

a) Do not accept friend requests from unknown people on social media platforms. A cyberbully can even create a fake account to befriend children. As a rule of thumb, only add people online who you know offline.

b) Remember what you post online remains there, so do not share your personal information like date of birth, address, and phone number on social media or other online platforms. You can go to privacy settings on social media platforms to select who can access your posts online. Try to restrict access of your profile to your friends only.



Think
Before you post

Is it..... **TRUE?**
Is it..... **HURTFUL?**
Is it..... **ILLEGAL?**
Is it..... **NECESSARY?**
Is it..... **KIND?**

How to stop
CYBERBULLYING

1
LOG OFF
the site where bullying is happening

2
BLOCK EMAILS OR MESSAGES.
Dont respond to them.

3
SAVE THE MESSAGE OR EMAIL
and show it to an adult.

4
TELL SOMEONE
you trust



STOP THE HATE
Always respect each other online,
even when you disagree with them.
#EndCyberBullying

c) Do not install unwanted software and apps like dating App, online games, etc. from unknown sources. Be careful of revealing personal details or identity details if using common spaces for online interactions.

d) If you feel upset after reading a post from a friend or a stranger, do not react with an aggressive reply. Resist the urge to retaliate or respond immediately. It may encourage the bully to keep posting such messages. Take a break and do something you enjoy doing to distract yourself.

e) Convey your discomfort to friends and acquaintances about hurtful posts or messages they may have shared or sent with unequivocal request to not to do it again. If such posts and messages persist, inform your parents or trusted elders immediately so that they can support you.

f) Block and if need be report using the site's reporting function as soon as possible if someone makes you uncomfortable on a social networking site.

Cyberstalking is when an individual is repeatedly or constantly followed, watched or contacted through any electronic means. The movement of the child is tracked and privacy is invaded or persistent efforts are made to contact someone against their will through text, email, social media, or other digital platforms.

Cyberstalking a child may be directed at sexually harassing a child or for other malafide motives. It could be done by an adult or an older child.



Causing harm to somebody unintentionally through the use of technology.

Unintentional Harm:

Cyberbullying has an adverse effect on the victim and can cause emotional and psychological problems. Victims can experience stigmas, shame and humiliation from peers. Often they may report headaches, stomach aches that often accompany nervousness and anxiety. They may also turn to self-harm in different ways. Being bullied can lead to low self-esteem and poor performance in school. In some cases it can lead to depression with some children feeling hopeless and helpless about their lives. In extreme cases it can lead to suicide by the victim.

Just think. Would you like to be at the receiving end for these possible consequences, even if these are unintentional? Consider the possible impact of your online actions. You may cause a lot of harm to the child which can have a long term impact on personal well being as well as school performance. Will you be comfortable being responsible for any of this?



What To Do When You Realise You Are Experiencing The Impact Of Cyberbullying / Cyberstalking?

If a child has been the victim of cyberbullying or cyberstalking and/or is experiencing any of the signs of harm described above, the child must immediately inform a trusted adult, either parent, teacher, counsellor or relative. They will initiate the actions required for addressing the offender as well as take measures to provide help for coping with the ill effects. This is in your interest; do not remain quiet about it. Remaining quiet will give the offender confidence to trouble other children as well. At the same time you will ignore your need for help and assistance to cope with the situation.

A class 10th girl was getting lewd phone calls and messages from some anonymous number. She was afraid to tell it to her parents because she knew her dad was hot tempered and would try to harm the anonymous caller by tracking him down. With this fear this fear in her mind she didn't bother to complain. The phone calls and messages didn't stop. She started fearing that the boy can follow her too and sooner did this happen. Wherever she went, he started following her, be it her tuition classes, be it some outing spot. The situation became worse when he started clicking her pictures. The girl was frightened and she dared to complain to the cybercrime branch.

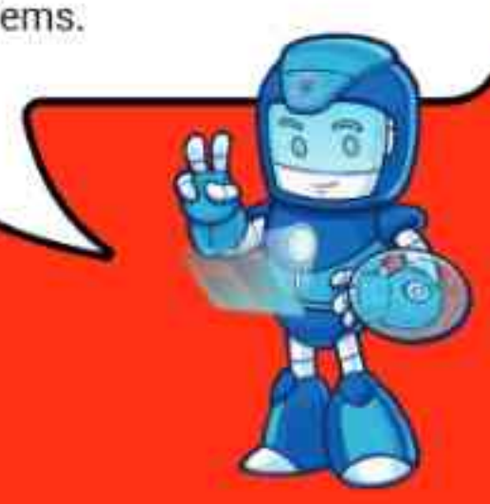
Lesson: Always tell your parents or a trusted adult if someone is troubling you. They would be able to help you. Take the screenshots of such chats as proof, which can be shared with the police authorities.





A girl of class 9th was abused and threatened by a relative. She was tortured and sometimes even drugged. The relative used to send her abusive messages and threaten her that he will tell her parents that she has a boyfriend. She was scared to confide in her parents because of the fear that her parents would not believe her.

Lesson: Keeping silent is not a solution to such a problem. Never be scared of telling your parents the truth. Make sure to complain about such problems to the police and seek help from authorities whenever needed. There are people willing to listen to you and help in addressing your problems.



A 7th standard girl was blackmailed by an adult who kept on asking the girl for her nude pictures. She explicitly refused every time he asked and blocked the person. The blackmailer hacked one of her social media accounts and took her photos and just to take revenge he morphed her photos and posted them online. The girl was embarrassed, agitated and even thought of committing suicide.

Lesson: Be strong and face the situation wisely. Do not be afraid of such offenders. Report such crimes on the social media platforms, cybercrime branches, authorities who work for child development, child helpline. Do not think of yourself as a victim.



5.5 TEACHER ABUSE BY CHILDREN

A recent trend observed is that some children are taking to online platforms to take revenge on their teachers either by posting derogatory comments with the name of the teacher in a group, starting a discussion about them which attracts

other negative comments, posting explicit pictures or stalking either by impersonating someone or through unauthorized access to teachers devices. All these activities are unethical and against digital etiquette and at the same time, several of these may attract legal consequences.

If students have issues concerning their teachers, which are bothering them, they should approach the school administration rather than resort to such measures that can get them into serious trouble.

5.6 ONLINE REPUTATION AND DIGITAL FOOTPRINTS

Internet users leave behind "digital footprints", which can influence their reputation. It is made up of the content created, posted and shared by the user, as well as the content posted and shared by others with and about the user. It is made up of information on websites they visit, emails they send, any information they submit online, and posts on social media platforms. It can be positive or negative and affects how people see the user now or in the future. So it is important that you know what kind of trail you are leaving, and what the possible effects of this trail can be.

Make a positive footprint: The best way to keep your online reputation in check is to use your time online to get creative and create a positive footprint. For example, why not write a blog to promote all the great things you are doing, fundraise for a charity using an online sponsorship page or create a video to teach others something new.

Many social media platforms offer insights into the personality traits to the users. Their interest is expressed once they accept the offer or take a related quiz. They give their consent in this process or their consent is deemed. The social media platform and/or the app developer are able to use the information trail left by the user to offer them the results. This is indicative of the amount of information about the users that the social media platforms possess.



University Case

Kyle Kashuv, a recent graduate of a high school in Parkland, Florida in the US gained initial notoriety as an outspoken advocate against gun control in the wake of the 2018 Parkland attack that left 17 dead. He had survived the incident but unlike many of his classmates who demanded stricter gun control measures, he argued for maintaining strong Second Amendment rights and successfully lobbied for the federal STOP School Violence Act, which included several school safety measures in lieu of stricter gun control measures. According to his classmates, he was prone to expressing vile, blatantly sexist and racist views in person, texts and shared google document. Not only did Kashuv become something of a celebrity, he also was very academically accomplished and won admission to Harvard.

But in May, the Huffington Post released a series of vile, blatantly racist slurs made by Kashuv after receiving them from Parkland students. Although Kashuv attempted to delete the document, it was too late. He posted a Twitter explanation for what he called "callous comments I made a few years ago," claiming "we were 16-year olds making idiotic comments, using callous and inflammatory language in an effort to be as extreme and shocking as possible. I'm embarrassed by it, but I want to be clear that the comments I made are not indicative of who I am or who I've become in the years since."

Almost immediately, Harvard launched an investigation, including contacting Kashuv for an explanation and informing him that it reserved the right to withdraw offers of admission in situations where students behave in ways that "brings into question your honesty, maturity or moral character." Kashuv sent a letter of formal apology to Harvard, but the university decided to rescind his admission and rejected his appeal against its decision on the basis of reports and his written sentiments.

The reaction to Harvard's decision to withdraw its offer of admission to Kashuv was strong and loud. One perspective was that a liberal institution treating a conservative youth unfairly. After all, he was only 16 when he stated his racist views and had subsequently apologized. The other perspective defended Harvard's decision as a proper and necessary institutional rejection of racism. College admissions are premised on the behaviour of young people. As a private university, Harvard has every right to decide which students will be admitted.

Source: Various media reports. See: Adam Harris "Harvard's Drastic Decision" in The Atlantic. June 17, 2019.
Retrieved from: https://www.theatlantic.com/education/archive/2019/06/harvard-rescinds-admissions-offer-kyle-kashuv-racist-remarks/591847/

Protect Your Online Reputation

Use the simple checklist to help manage and maintain your online reputation.

Search Yourself Online: Do you know what information about you is available online? Do a simple web search of your name and see what you can find. If you find something you are not happy with, take the necessary steps to get that content removed. Remember if your Facebook or Twitter pages appear you can change this by adjusting your privacy settings.

Check Privacy Settings: Make sure you know what information you are sharing on the websites you use, in particular on social networking sites. Most social networking sites have privacy settings to help you manage the content you share and who you share it with; you can decide if you want your posts to be shared with your online friends and followers only or with the public. Keep in mind that your friend's content and their settings can also affect your digital footprint.

Think before you post

Before you post that funny picture of your friend, or make that joke about someone on Twitter, ask yourself do you want everyone to see it; friends, family, grandparents, future employers? Would you be happy for others to post that type of content about you? You should be proud of everything you post online, remember once it is online it could potentially be there forever!



Deactivate and delete: when you stop using a social networking profile or website, it's a good idea to deactivate or delete your account. This will mean the content is no longer live and should not be searchable online; it will also remove the risk of these accounts being hacked without you knowing.

Cambridge Analytica came under media glare and public scrutiny when it was revealed that it was selling psychological data to candidates in the US Presidential election. The revelations have placed the practices and responsibilities of Facebook and other companies under intense scrutiny, and raise questions regarding the responsibility of the Internet industry.

Cambridge Analytica case and its implications for data privacy

Political data firm Cambridge Analytica obtained the data of 50 million Facebook users, constructed 30 million personality profiles, and sold the data to US politicians seeking election to influence voters, without the users' consent. The following are some facts of the case.

A Cambridge University researcher developed an app called 'thisismydigitallife' in 2014. The users had to consent to give the app access to their Facebook profiles and those of their friends in order to take the quiz. They were to receive $1-$2 to take the quiz, which was advertised to remote freelance workers on Mechanical Turk, a crowdsourcing online marketplace controlled by Amazon.

Over 270,000 users took the quiz. But the app was able to access the full profile of over 50 million friends' accounts which, at the time, Facebook's API (application programme interface, i.e., the platform for building applications) allowed by default. The researcher obtained a licence from Facebook to harvest such data through its API 'for research purposes only'. But he violated this agreement by giving the data to political data firm Cambridge Analytica, which was co-founded by a donor to the Republican Party in the US, and which reportedly paid him $7 million for his efforts.

Cambridge Analytica matched the data of 30 million users (out of the original 50 million) with other records to construct personality profiles on millions of American voters. It classified voters using five personality traits - openness, conscientiousness, extraversion, agreeableness, and neuroticism (OCEAN) to identify the personalities of American voters and influence their behaviour, using psychographic modelling techniques.

In December 2015, the media found out that Cambridge Analytica had sold psychological data to a candidate in the US presidential campaign. It was reported that

facebook claimed that it had removed the app once it learned of the violation of platform policies. But did not clarify what it did with the information that had already been gathered. The researcher, Cambridge Analytica, and one of its former employees certified to Facebook that they had deleted the data. But Cambridge Analytica continued to sell the data to another candidate.

The investigations are going on with allegations of Russian interference in the US election and ties with the group behind the UK's Leave EU campaign (Brexit) in 2016. It has been reported that a large amount of the data is still on the company's servers even though it is not clear how much the data actually contributed to influencing voters.







ACTIVITY 1

There is a fine line between cyberbullying and cyberstalking.

Cyberbullying

Cyberstalking

ACTIVITY 2

What all should not be posted online?

- [ ] DOB
- [ ] Verified news
- [ ] Private Photos
- [ ] Mobile Number
- [ ] Location
- [ ] Personal Details
- [ ] Mean/Hurtful comments
- [ ] Forwarded spam messages





What precautions must be taken while sharing information for legitimate purposes with known and trusted persons, which should otherwise not be posted online.

ACTIVITY 3

Write down at least seven digital etiquettes.

ACTIVITY 4

List various forms of cyberbullying.



ACTIVITY 5

How can you protect your online reputation?

06 DIGITAL HEALTH AND WELLNESS

6.1 WHAT IS DIGITAL HEALTH AND WELLNESS?

Digital health and wellness is the ability to use technology like mobile phones, laptops, desktops and tablets and not using too much till the point where it hurts. Excessive and improper use of technology could lead to lifestyle changes that affect everyday life negatively.



6.2 OPPORTUNITIES AND RISKS

Mild use of digital technology is beneficial while excessive use can have a negative impact.

Physical Health Problems And Obesity: As time spent on digital technology increases, time spent on physical activity is reduced, which might be a contributing factor to child and adolescent physical health problems. Lack of physical activity could be detrimental to the health and well-being.

Limited Movement Of Limbs: When people spend countless hours daily hunched over numerous types of handheld devices with their heads bent forward, they are at risk of developing "text neck." Complaints associated with text neck are neck, back, arm, finger, hand, wrist and elbow pain, as well as headaches and numbness and tingling of the upper extremities. There is a chance of developing shoulder complaints.

Eye Strain: Eye redness or irritation from staring at the bright backlight of screens for long periods, dry eyes due to reduced blinking, blurred vision and general fatigue from staring at screens and straining to see small fonts and images are all symptoms of digital eye strain.

Hearing Loss: Prolonged exposure to high volume sounds, especially with ear plugs and phones, can contribute to hearing impairment. You can keep your hearing intact by following the 60/60 rule.

Listen to any device at a maximum of only 60 percent of its full volume for a total of 60 minutes a day. By taking this advice as an early warning, we can protect the hearing that we have now, and carry on enjoying the wonders that sound brings to life.

Accidents: Avoid use of online activities like selfie, social media use or any other online activities to avoid accidents while you are on the move. Traffic rules also have made this a punishable offence and invite fines. While it is good fun to get good pictures to capture the moment, do not allow the social media obsession for the 'perfect' selfie, or the number of likes you get, influence your judgement or affect

your self-esteem or force yourself to compare yourself with others.

Abuse And Addiction: Excessive use may not be addiction. If the user is using digital technologies for genuine purposes, e.g., home work, research, essential communication and moderate leisure, and does not hamper other routine activities, the time spent online may be justified.



Evaluate Your Own Online Use By Asking These Questions:

- Do you check the phone first thing upon waking in the morning?
- Do you check your phone frequently throughout each day?
- Do you have a hard time unplugging at night?
- Do you look at the phone while in conversation with friends or family?
- Do you picking up the phone whenever you are bored?
- When offline, are you preoccupied with getting back online?
- Do you forget doing homework or other household tasks for being on the Internet?
- Have you lost all interest in the activities you used to enjoy and spend a lot of time online?
- Are your online activities stopping you from spending time with friends and family?
- Do you prefer being online than being around real, live friends and family?



- Do you seek new friendships with people met on the Web?
- Does the number of friends, likes and views on social media affect you?
- Is your academic performance in school getting affected?
- Are you learning something related to your goals in life through your online activities?
- Is your online time contributing to your school assignments, career goals, and entertainment?
- Is your online time contributing to your hobbies or special interests?

By answering these questions you should consider whether you need to be conscious you are getting too absorbed in the technology and it is affecting your normal activities, relationships and life and career goals and you need to regulate your online time and activities.

Discussion and negotiation with adults, e.g., parents, guardians and teachers, do help in identifying if the quantum of use is excessive. But over a period of time, increasingly excessive use of digital technologies can lead to addiction.



Nomophobia

"No Mobile Phone Phobia", is the irrational fear of being without your mobile phone or being unable to use your phone and the services that the phone provides (especially phone calls and Internet connection) for some reason, such as the absence of a signal or running out of minutes or battery power. A phobia is by definition an irrational fear."

The WHO has recognised "gaming disorder" or a "pattern of persistent or recurrent gaming behaviour" in which people lose control of their gaming behaviour, give priority to gaming over other interests and activities, and continue gaming despite negative consequences, such as impairments in their family relationships, social lives, studies or work or other areas as a mental health condition.

Real versus virtual life: Appreciate the distinction between real life and virtual life. How many "likes" and "shares" a social media post receives is not an indicator of popularity, or personal worth, which should influence self-esteem. The "fear of missing out" or FOMO can be a strong driver, especially when others in school or friends circle share images on social networks and can create a strong pull to be part of the 'in' crowd. The principle of YOLO or "you only live once" reinforces the hedonistic idea that the one life one has is meant to be enjoyed. But there is a very fine line between trying new things and endangering yourself. With new online challenges and trends coming up every day, make sure you keep in mind your safety first.

Cyberbullying is known to cause depression, social anxiety, and diminished quality of family and social relationships. It may also lower academic performance and push the victim to risky behaviour. It can be prevented with some help, motivation and courage. Cyberstalking causes stress, anxiety disorders, fear and psychological trauma regardless of the fact whether the victim actually meets the harasser or not and experiences a feeling of helplessness and maybe lack of support.Change in eating and sleeping patterns may also be observed.It is advisable to immediately inform a trusted adult if such an incident occurs and seek help and not keep quiet about it.



6.3 GOOD PRACTICES

6.3.1 Everything In Moderation

Anything used in excess is harmful therefore it is essential that a balance between online usage and other tasks such as school assignments, social interactions and outdoor activities is maintained.

Time limit for the use of digital devices. Setting limits for the time spent with mobiles, laptops, desktops and tablets enables the user to do other important things and lead a balanced and fulfilling life.

Setting screen time. Are you in the habit of constantly checking notifications? Do you constantly wonder whether your contacts have read your messages?



6.3.2 Periodical Digital Detox

Find certain moments to disconnect yourself from a mobile phone. Switching off while having meals and sleeping, and setting "no mobile" or "silent mobile" time slots are not only good but necessary. Place your phone at least 15 feet away from you when you sleep at night. Keep it silent and resist the temptation to check it before the morning. Turn off the mobile phone while having conversations and interactions with people.

Aerobic exercise will help to sustain strength, improve cardiovascular conditioning, and counteract the strain of sedentary computer use.

6.3.3 Sound Ergonomic Practices

Simple ways can prevent possible harms resulting from the continuous use of mobile phones, laptops, desktops and tablets.

Alternate tasks to make changes in your working position to avoid making the same movements for prolonged periods of time. Prolonged use of a computer keyboard and/or mouse can cause muscle aches and nerve pain. Customize your computer to maximise comfort and efficiency by using your software. Adjust the screen font, contrast, pointer size, speed, and colour of the digital devices.

(A) Posture

Maintain good posture when working at the keyboard. Sitting on a chair with back support is helpful.

- **Neck and trunk:** Avoid twisting or bending them. Avoid excessive reaching. Position frequently used items directly in front of you and angled upward on a copyholder when working.
- **Shoulders:** Keep your shoulders relaxed with your elbows close to your sides.
- **Feet:** Keep your feet supported on the floor or on a footrest when you work to reduce pressure on your lower back.
- **Elbows:** Avoid resting your elbows on the hard surface or edge of your table. Use pads to protect your elbows if necessary. Elbows positioned at 100 to 110 degrees when working help with a relaxed position at the keyboard. Elbows should be positioned at 100 to 110 degrees when working in order to keep a relaxed position at the keyboard. This could require a slight negative tilt (front of keyboard higher than back) when working in upright positions. If reclined in your chair, the keyboard could be at a positive angle to maintain this relaxed position.
- **Wrists:** Your wrists should be in a neutral or straight position when keying or using a pointing device or calculator. Wrist rests can assist you in maintaining a neutral position when used properly during pauses. Float your arms above the keyboard and wrist rest when keying. Avoid planting your wrists on the table or wrist rest. This can result in bending the wrists either up and down or side to side.
- **Hands:** Your hand should be relaxed. Keep your fingers and knuckles relaxed when working at the keyboard. Avoid holding your pointing device tightly. Never hold a pen or pencil in your hand when keying. Avoid hitting the keyboard with excessive force. Studies have shown that the average user hits the keyboard with four times the required force when keying.
- **Eyes:** Blink your eyes frequently while focusing on the screen. Rest your eyes by refocusing on distant objects intermittently when working. Take a one or two-minute break every 15 to 20 minutes, or a five-minute break every hour to stretch your limbs. Every few hours, get up, move around, and do an alternative activity.



WATCH

https://www.youtube.com/watch?v=9LgsWRacnuk&t=3s

(B) Positioning

a) When writing at the computer, avoid excessive reaching over the keyboard or work materials. Your keyboard, pointing device, files and telephone should be within easy reach. A sturdy in-line copyholder can double as a writing surface if appropriately positioned.

b) Use a keyboard tray to properly position your keyboard and pointing device.

c) Use a copyholder positioned in line with your monitor and keyboard.

d) Position the monitor so that the viewed part of the screen allows you to keep your neck in a neutral or straight position. The monitor should be centred directly in front of you. The top of the computer screen should be slightly below the top of your head, so that you are looking at it with a slightly downward gaze.

e) Position your monitor to eliminate excessive glare or reflections from windows and lighting.



https://www.ehs.pitt.edu/workplace/ergo-tips.html

You can also reduce strain by using features like swiftkey which will help you type faster and more easily by simply sliding your finger on you phone keyboard. You can also use the option of "Sticky keys" on PCs to create shortcuts and make your work easier.

Use Only The Apps That You Really Need.

a) Installing an endless number of apps (especially social networks) on your mobile phone can be a total trap. While communication options multiply, a person suffering from nomophobia needs to feed their addiction even more. Therefore, not installing that many applications can be a good way to avoid the temptation.

b) In order to feel liberated, try a technology fast every month where you actually go for a day or more without a computer, tablet or phone.

Technology should improve lives and not enslave the users. That is why, using technology in a reasonable way will always be the smart choice. And if you are not able to do it by yourself, do not hesitate to ask for help.

6.4 SHARING PROBLEMS TO SEEK SOLUTIONS

Talking about the problem can be the first step to solving it. If something upsets you online or you are worried about a friend it can really help to talk to someone. There are lots of people who can help you, such as friends, family members and teachers. Talk to an adult who you trust. Talking about a problem can often make you feel better. If you keep your worries to yourself they can grow. It is a lot easier to solve a problem when there are two heads working together on it.

Often we do not talk to our friends or parents about the things we would like to because we feel embarrassed, shy or ashamed. The thing to remember is that whatever it is you are embarrassed about; a good friend is not going to laugh at you or put you down. They will listen, try to understand and try to help you feel better or find a solution. And that's why people find that talking to a good friend about a problem usually does help.



The services that you use online should also offer a reporting service, such as being able to talk to a moderator or report other players. It is important that you talk to an adult you trust if anything has upset you or made you feel uncomfortable whilst online. Remember you can always call ChildLine on 1098.

Peers: Communicate with your trusted friends, especially those who know more about the problems or have had similar experiences, without the fear of being judged. However, a certain level of knowledge and sensitivity is required for solutions so do approach an adult who has your trust for advice and support.

Parents: Speak with and seek help from parents if some kind of "family agreement" has been arrived at through dialogue within the family.

School counsellors or teachers.

If your school has a counsellor, discuss your problem with them. They are there to answer your questions and provide guidance and assistance. You may even approach a teacher or school staff who you trust and feel comfortable speaking with.

Seeking help from experts.

Professional expertise is available, although not everywhere, to assist with various problems related with misuse or excessive use of digital devices and technologies.

The following institutions are well-known for their expertise on digital health and wellness.

a) SHUT clinic (Service for Healthy Use of Technology), National Institute of Mental Health and Neurosciences (NIMHANS), Bengaluru, Karnataka.

b) Department of Psychiatry, the All India Institute of Medical Sciences, New Delhi.



Open discussions and family agreements

Although the risk of abuse online is clearly serious, the capacity of most children (and their parents) to protect themselves is often under-estimated. Open and informed discussions among parents and children about the internet from an early stage can be the best defence against online grooming and bullying.

Parents often seek the security of their children but they should not be snooping, which can leave children feeling untrusted and increase the risk of self-harm. Ideally, a family agreement is a good way to start a conversation with the whole family about how everyone will use the internet and discuss together how to behave in a positive way when online at home, at school or at a friends house.

WATCH

https://www.youtube.com/watch?v=5HtkGAm2kbg

ACTIVITY 1

Research online or offline to make a list of good practices to prevent and reduce the following problems associated with excessive use of digital devices.

I. Eye strain :

II. Backache :

III. Carpal tunnel syndrome :



07 DIGITAL RIGHTS, FREEDOMS AND RESPONSIBILITIES

7.1 WHAT ARE DIGITAL RIGHTS?

Digital rights are basically human rights in the digital era, when internet is increasingly being regarded as a right rather than a luxury. The rights to online privacy and freedom of expression are really extensions of the equal rights laid out in the **United Nations Universal Declaration of Human Rights.**

According to the United Nations, disconnecting people from the internet violates these rights and goes against international law. Digital rights include access and participation, free speech, community, privacy, physical and psychological safety, safety of identity and of material and intellectual property. **But as Uncle Ben said in the Spider Man, "with great power comes great responsibility."** The responsibilities include knowing and respecting the community standards and guidelines of all social media, video platforms and online groups being used and staying within the parameters of these guidelines.

If any activity violates the community guidelines of a social media platform, the post, comment, photo, video or even the account can be deleted.

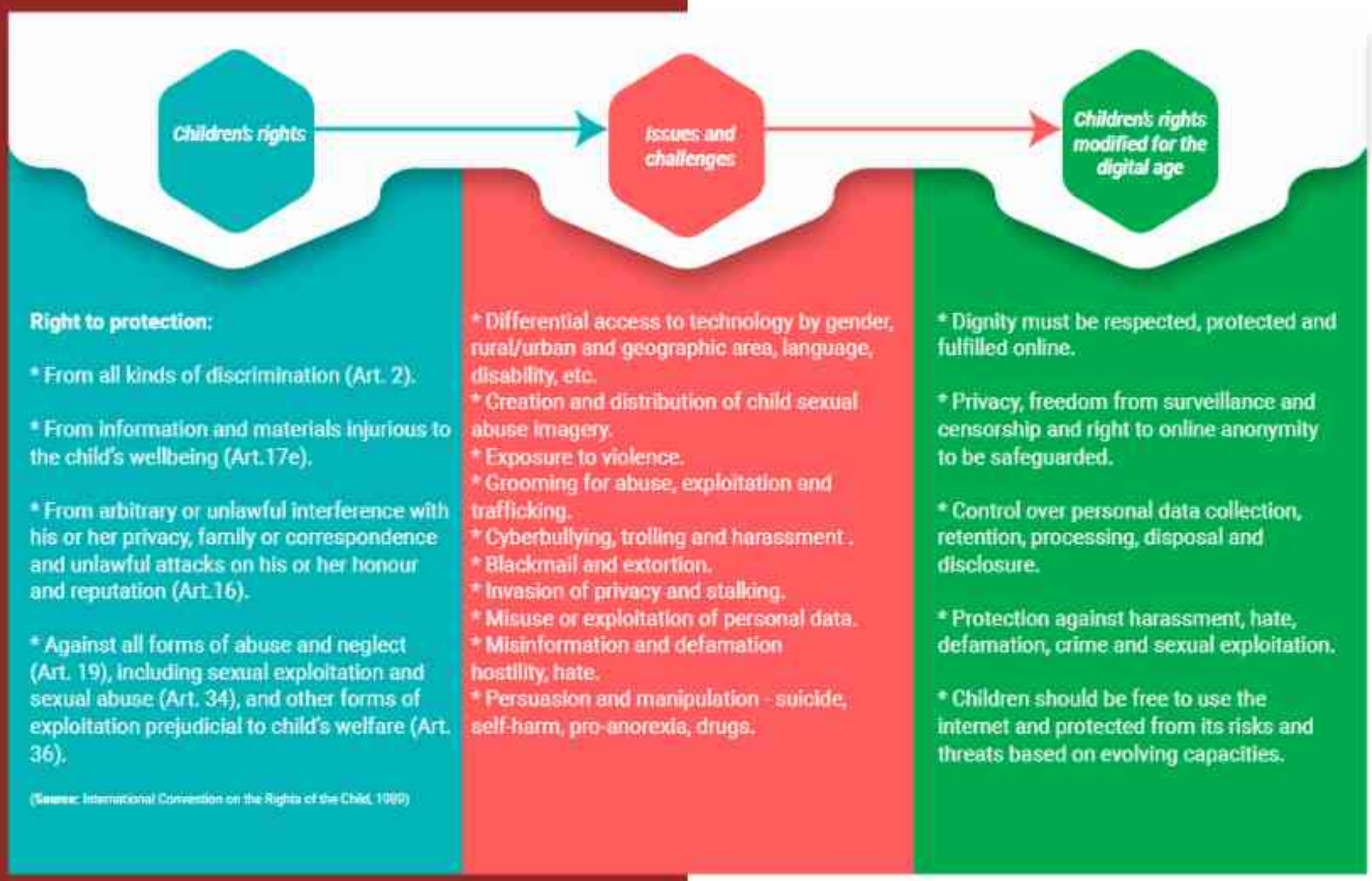
Snapchat Community Guidelines :
https://www.snap.com/en-US/community-guidelines

Instagram Community Guidelines:
https://help.instagram.com/477434105621119

Facebook Community Guidelines:
https://www.facebook.com/communitystandards/

WhatsApp Community Guidelines:
https://www.whatsapp.com/legal/

Twitter Community Guidelines:
https://help.twitter.com/en/rules-and-policies#general-policies



Children's Rights	Issues and Challenges	Children's rights modified for the digital age
PROVISION: To support children's right to life and development (Art. 6) To preserve his or her identity (Art.8) to education to support development of his or her full potential (Art.28) and prepare them for a responsible role in a free society (Art.29) to recreation and leisure appropriate to their age (Art.31) to diverse material of social and cultural benefit to the child (including minorities) to promote children's well-being (Art. 17) to all measures for recovery from neglect, exploitation and abuse (Art. 39).	* Formal and informal learning resources and curriculam. * Wealth of accessible and specialised information. * Opportunities for creativity exploration and expression. * Digital skills and literacy. * Ways to counter inequalities. * Expanded entertainment choices. * Access to cultural and heritage content online in an equitable way.	* Life, liberty and security. * Access and use of a secure and open internet, including addressing special needs of disabled children. * Cultural and linguistic diversity on the Internet must be promoted and innovation should be encouraged to facilitate plurality of expression. * Education through the internet, to culture and knowledge online.
PARTICIPATION: In all actions concerning children... the best interests of the child shall be a primary consideration (Art. 3), including the right of children to be consulted in all matters affecting them (Art. 12); see also child's freedom of expression (Art. 13) and freedom of association and assembly (Art.14) to information (Art.17) and to participate fully in cultural life (Art.31).	* Enhanced networking opportunities. * Ways of consulting children in diverse situations and processes including consulting them on education, research and online issues. * Platform for children's voices. Child-led initiatives for local and global exchange * Peer to peer connections for sharing and collaboration. * Recognition of rights and responsibilities.	* The internet is a space for promotion, protection and fulfilment of human rights and advancing social justice, including for all children. * Seek, receive and impart information freely and to associate freely with others for social, political and cultural purposes.

Table adapted from UNICEF and Child Rights in the Digital Age by Sonia Livingstone

The UN Committee on the Rights of the Child is in the process of finalising a General Comment on Children's Rights in relation to the Digital Environment, which will provide global guidance to all countries on how different stakeholders can take measures to protect children's rights.This will become available shortly on the following website:

https://www.ohchr.org/EN/HRBodies/CRC/Pages/CRCIndex.aspx

DO YOU KNOW YOUR RIGHTS?

Right To Education

The right to education has been recognized as a human right in a number of international conventions, including the International Covenant on Economic, Social and Cultural Rights which recognizes a right to free, compulsory primary education for all, an obligation to develop secondary education accessible to all, on particular by the progressive introduction of free secondary education, as well as an obligation to develop equitable access to higher education, ideally by the progressive introduction of free higher education.



The Right To Privacy

As discussed Article 21 of the Constitution of India states that "No person shall be deprived of his life or personal liberty except according to procedure established by law". The right to life enshrined in Article 21 has been liberally interpreted so as to mean something more than mere survival and mere existence or animal existence. It therefore includes all those aspects of life which makes a man's life more meaningful, complete and worth living and right to privacy is one such right.



Right To Be Forgotten

The right to have data about oneself erased or withdrawn by service providers is the right to erase the past unwanted history of a user by the social media and search engines, is an evolving concept which is being discussed in several fora. While legal experts are advocating the right to be forgotten strongly in the context of privacy rights, it would take quite some time before an agreement is reached globally on its scope and modalities.

Personal information that you share can be used against you. Review the content that you wish to share online and only provide information that is essential and absolutely necessary.



Right To Be Safeguarded From Violence, Abuse And Exploitation

Children have a legal right in international and most domestic law to be safeguarded from abuse, including sexual abuse. The legal responsibility is on the government to prevent abusers from contacting children. The government needs to take all measures to make the internet as safe as possible an environment through measures to prevent the creation and distribution of online child abuse imagery, sexual grooming, and online dimension of child trafficking.

Right To Freedom Of Expression And The Right To Be Heard

The freedom of speech and expression is regarded as first condition of liberty. It occupies a preferred and important position in the hierarchy of the liberty, it is truly said about the freedom of speech that it is the mother of all the other liberties. In modern time it is widely accepted that the right to freedom of speech is the essence in the society and it must be safeguarded all the time. The first principle of a free society is an untrammeled flow of words in a open forum. Liberty to express opinions and ideas without hindrance, and especially without fear of punishment plays significant role in the development of the particular society and ultimately for the state. It is one of the most important fundamental liberties guaranteed against state suppression or regulation.



Children's Rights To Leisure And Age Appropriate Recreation

Children have a right to recreation and leisure as appropriate to their age, an education that will support the development of their full potential and prepare them for responsible life in a free society. To ensure this right, the government and educational authorities have to take measures to provide educational technology, online information and creative resources and promote digital skills equitably, factoring in differences in languages, access or conditions of disability or disadvantage.



The Right To Intellectual Property

In principle, children have the right to intellectual property. The Indian Contract Act prevents minors from entering into a contract but permits the claim of intellectual property rights for their original creations through the legal process of claiming copyright.

Most social media websites, including YouTube allow children above the age of 13 to register. However, parental guidance and monitoring is a must because the norms and policies of websites need to be vetted carefully.

Children's Right To Participation

This right includes the right of children to be consulted in all matters affecting them, which is seen in conjunction with the child's freedom of expression, and freedom of association. The government and its agencies, service providers, educationists and school administrations and civil society organisations are expected to provide children and young people for their inclusion in diverse societal processes, including consulting them on matters related to their education, research and ICT governance when it affects them.



Have you ever participated in any discussions in your family and school about responsible use of digital devices and internet?

The Right Of Access To Redress And Justice

Children have a right to justice. Ensure that children have avenues for formal, including legal complaint in cases where their online rights have been breached and the support to make effective use of these complaints procedures. Children have to be made aware of all these provisions and how to use them if required. They also need to know who to go to for guidance and support.



https://www.youtube.com/watch?v=5ubyLUgBEF4

WATCH

ACTIVITY 1

If you find yourself in the following situations, which right would you exercise.
Match the following :

Situations ?		Rights
A family friend is blackmailing you into sending inappropriate images to him.		
Your friend posts a picture of you without consulting you. When asked to remove the picture they refuse.		B Children's right to leisure and age appropriate recreation
On social media you have someone who stalks you and you want to make a complaint.		C The right to education and access to information
A sport organisation does not let you apply for its online cricket training programme because you belong to a lower socio-economic background.		D Children's right to participation
Your school library bans an educational book that is appropriate for your age group.		E The right to be safeguarded from violence, abuse and exploitation

A The right of access to redress and justice

ACTIVITY 2

Think of real life examples, which illustrate realisation or violation of your specific rights.



08 DIGITAL SECURITY

8.1 WHAT IS DIGITAL SECURITY?

Tools such as anti-virus software, biometrics and personal devices, e.g., the secure chip in a credit card or an ePassport are digital security devices because they offer freedom to communicate, work, travel and shop using your digital identity in a way that is secure.

Digital security is an all-encompassing term, which includes the tools to secure technology, assets and personal identity in the online and mobile world.



8.2 SECURITY OF DEVICES

Smartphones, laptops and tablets are all open to wireless security risks. Protect them against cyberattacks.

8.2.1 Common Threats To Devices

Viruses on digital devices are malicious programme codes that can corrupt the system and destroy the data within the computer.



Malware

Malware is a type of malicious software designed to gain unauthorized access or to cause damage to a computer **without the knowledge of the owner**, stealing and even deleting sensitive data, altering or hijacking computer functions to monitor users' computer activity.

Ransomware

Ransomware is a type of malicious software designed to **extort money from the user**. The attacker locks the victim's computer system files or blocks access to files or the computer system typically through encryption until the ransom is paid. **Paying the ransom is no guarantee that the files will be recovered or the system will be restored.**



Your One-Up about Hackers

A hacker is someone who will gain entry into a computer without permission, with the intention to use or exploit technology to cause harm, steal or destroy the data contained in it.

Usually hackers are well versed with computer technologies by using various applications or programmes that penetrate the defence mechanism employed by the target computer and send back the sensitive information like usernames, passwords, IP addresses and using them to gain access into the computer itself.

These applications or programmes can be in the form of Trojans, worms, malware and viruses, which will install in the system and compromise its security. **After all, if the hacker can gain administrative rights, they're free to do anything with the data contained in the compromised computer system.**

Several public locations like shopping malls and airports among others offer their customers free access to public Wi-Fi. But public Wi-Fi networks also enable cyber criminals to spy on unwary customers, take advantage of this convenience and intercept their data. They can access sensitive information of users' banking credentials, account passwords and other valuable information.

8.2.2 Preventing And Countering Threats And Risks

Install anti-virus software and ensure that is **updated as regularly as possible.** Some computers have built-in anti-virus software too.

a) Regularly update software and operating systems

Web browsers, plugins (Java and Adobe Products) and even Office Suites. It is the most common way hackers and malware try to gain access to devices and your information.

b) Use privacy settings on mobile phones, apps and browsers

Privacy settings on social media platforms enable you to select who can access your posts online. Try to restrict access of your profile to your friends only. Remember **what you post online remains there almost forever.**

c) Verify if the Wi-Fi link is legitimate and safe

Treat all Wi-Fi links with suspicion. Public Wi-Fi is inherently insecure – so be cautious. The Wi-Fi link could also be a bogus link set up by a cybercriminal trying to capture valuable, personal information from unsuspecting users. Don't connect to an unknown or unrecognised wireless access point. Try to use known Wi-Fi links, which are password protected.

d) Learn to create VPN to avoid downloading of data through public Wi-Fi.

Use your mobile phone to create VPN If you need to access any websites that store or require the input of any sensitive information consider accessing them via your mobile phone network, instead of the public Wi-Fi connection.

e) Verify if the website is legitimate/authentic

Avoid logging into websites where there's a chance that your identity, passwords or personal information may be compromised – for example, online banking services or any websites that store your credit card information.



f) Download apps from trusted sources like Google play, AppStore

g) Keep webcams private

These devices can sometimes be hacked and used to take pictures or videos of you without your consent. Put a sticker over your webcam, laptop camera, or phone camera when they are not in use.

h) USB Storage Device Use

• Always eject the device clearly to clear the content from your computer and to avoid damaging your data.

• Always scan the USB device with latest antivirus before accessing.

• Protect your USB device with a password.

• Encrypt the files/folders stored on the device.

• Use USB security products to access or copy data on your USB.

• Do not accept a promotional USB from unknown persons.

• Do not keep sensitive information like username and passwords on the USB.

g) Disable Bluetooth and Airdrop when not in use

Monitor your Bluetooth connectivity. Bluetooth is an amazing feature on many smart devices. However, leaving Bluetooth on while in public places can compromise your privacy. Bluetooth connectivity allows various devices to communicate with each other, and a hacker can look for open Bluetooth signals to gain access to your devices. Keep this function on your phone and other devices locked down when you leave your home, school, or similar secured area.

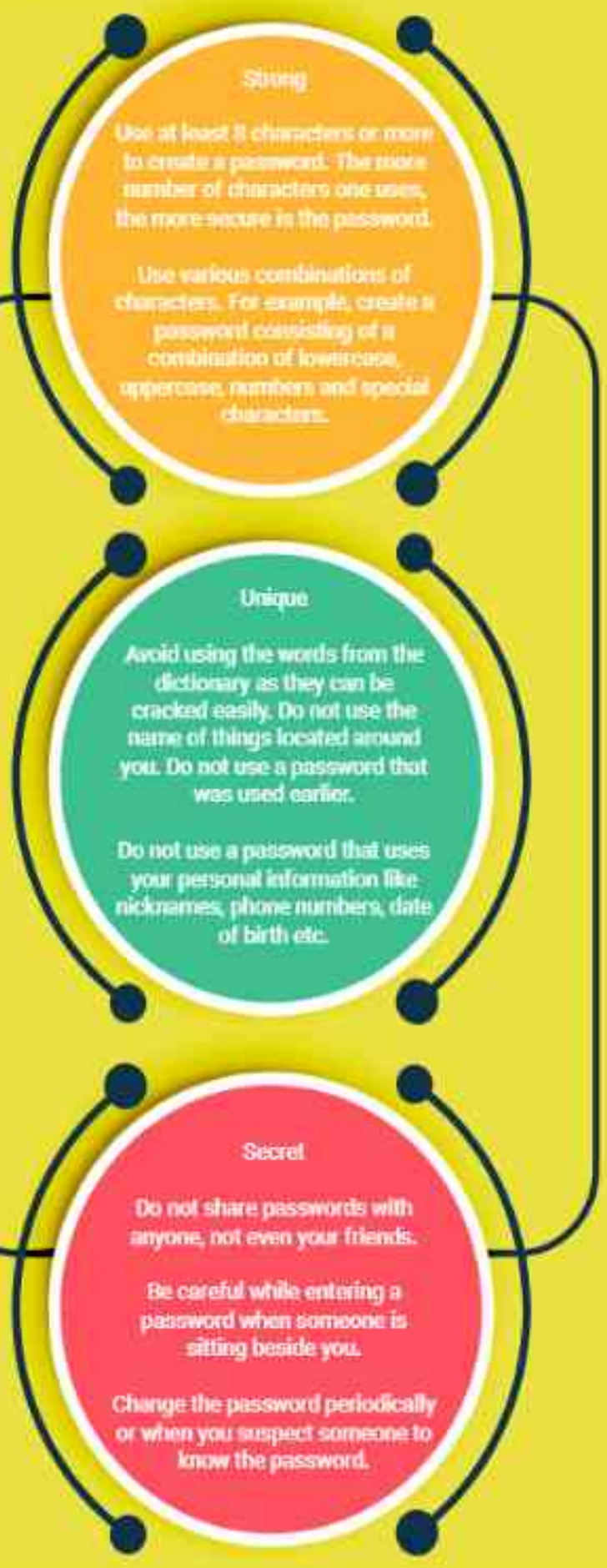
AirDrop feature allows you to send any kind of content like photos, videos, documents from one Apple device to another wirelessly. It doesn't impose any restrictions or limits on the file size. AirDrop makes use of the Bluetooth technology to detect and pair with other Apple devices which are located within the range of Wi-Fi and Bluetooth. It is highly recommended to turn on AirDrop only during file transfer.

8.3 OPERATIONAL SECURITY

8.3.1 Passwords

Strong, unique but easy to remember, and private passwords are essential for dealing with unauthorised access to online accounts. The passwords, when shared with other person(s), can be misused. They may be stolen by unauthorized users to collect and misuse your personal information.

Learn how to create strong passwords and passphrases. A password must be difficult to guess. But you should be able to remember it. Writing passwords somewhere is not advisable. Memorise it. Your password is given to you to maintain your privacy.



Go for an extra layer of security by opting for two-factor authentication (2FA), also known as two-step verification or dual factor authentication. This security process requires the user to provide two different authentication factors to verify themselves to better protect both the user's credentials and the resources the user can access.

Log out of your account when you plan to be inactive even for a short while. Always keep your system locked whenever it is not in use.



8.3.2 Emails And Messages

Most email providers offer filtering services.

The use of Rich Text Format instead of the standard .DOC format will retain the formatting but not any macros. This may prevent you from sending virus to others if you are already infected by it.

DO	DON'T
• Use email filtering software to avoid spam so that only messages from authorized users are received. • Scan the attachment with received messages with updated antivirus software before saving it. • Be very careful while downloading attachments from emails into your hard disk.	• Send personal information through emails. • Click on the emails received from untrusted users and the links that come via email.The act of clicking may execute some malicious code and spread into your system. • Open attachments with emails from strangers. They may contain a virus along with the message. • Send messages with attachments that contain executable code like Word documents with macros, .EXE files and ZIPPED files. • Fill forms that come via email asking for your personal information.

8.3.3 Security Settings On The Browser

• Update anti-virus software regularly.

• Adjust the settings in the web-browser. It may limit some functionality but can provide the best protection from malicious content.

• Enable email accounts for multi-factor authentication. Email is the gateway to almost every other account a user may have. When someone loses or forgets an account password, the reset is sent to his or her email.

• Gauge the credibility of the website by checking the URL, lock.

• Look out for warning signals given by web browsers about exposure to a malicious website or content. Such warnings can protect the user from malware, phishing and identity theft. These warnings given by most of the commonly used browsers like Chrome, Internet Explorer, etc. Remember to update your browsers regularly to avoid missing out on such updates.

• Exercise caution while giving details about personal information when registering for access to email accounts, social networks and chat rooms, and free game downloads.



Data Accessibility And Privacy

Certain online activities compromise the privacy of children.



Filling online forms for surveys, contests, downloading games on commercial or free websites. Some websites prompt the users fill-up their form for participating in games, surveys and contests. The name, email id, age and gender, and at times the telephone number and postal address, obtained in this manner can be used to access information.

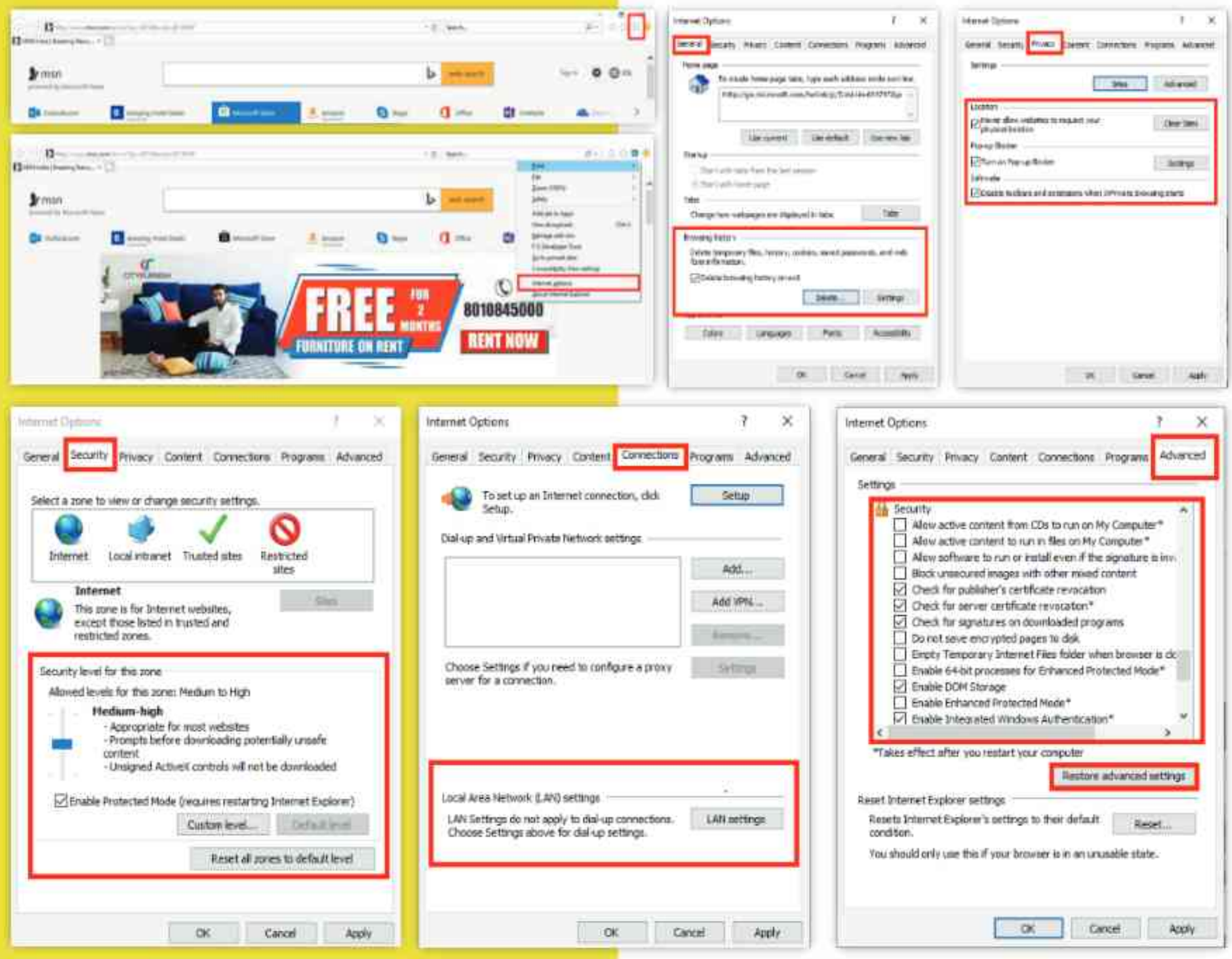
Some requests are legitimate: much depends on the nature of the website requesting the information. Providing personal information online can result in a student being targeted for spam (unsolicited email), advertising materials and/or viruses.

Privacy issues also apply to students developing personal websites and publishing online. Personal details, including photographs of themselves or other students, may lead to the information being captured and reused by others for illegal purposes.

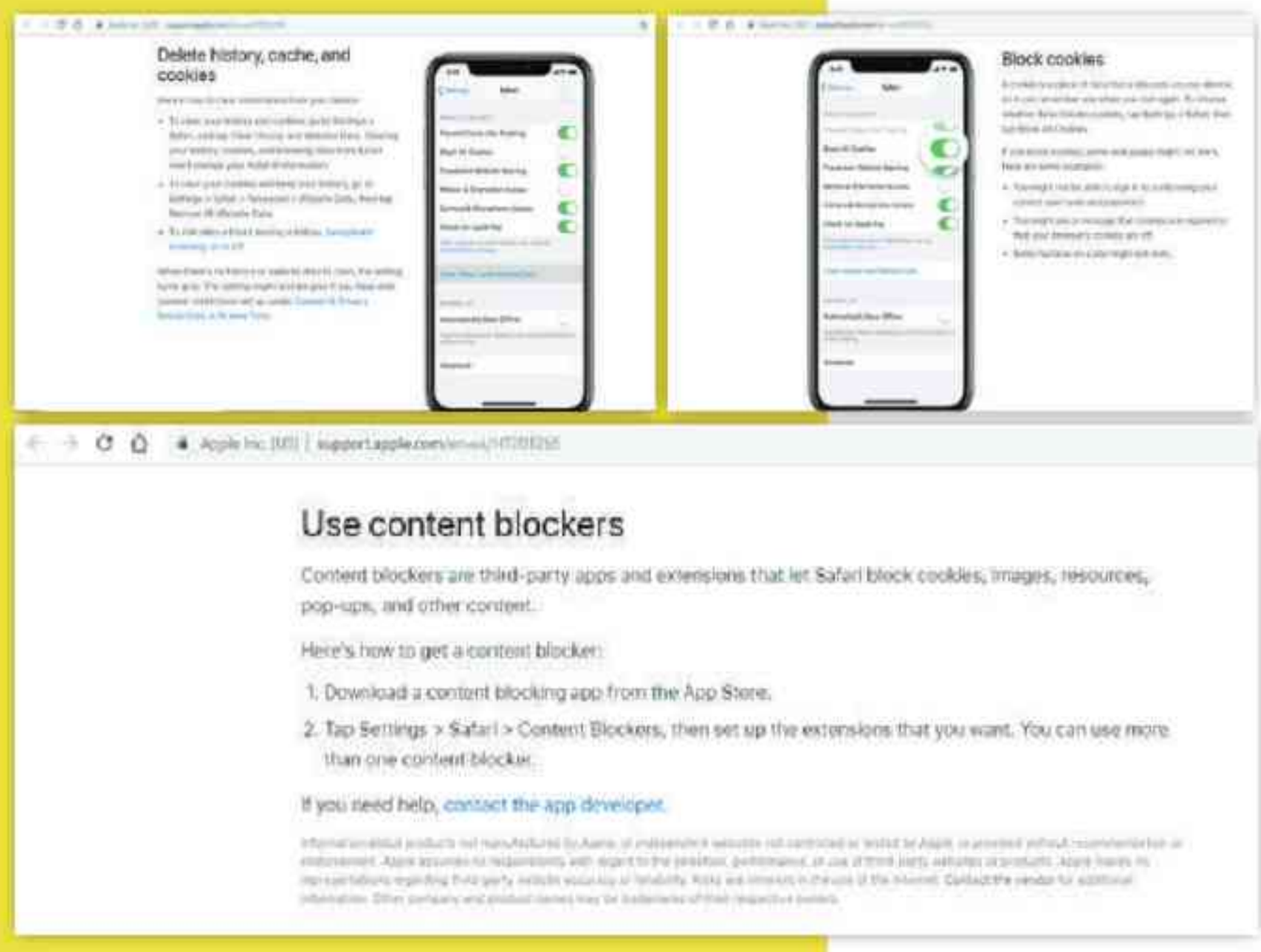
Use the following advice when browsing the web to reduce your risk of being a victim of cybercrime. Settings and security models are different for each browser. Visit the following vendor websites to learn more about the security settings in your browser.



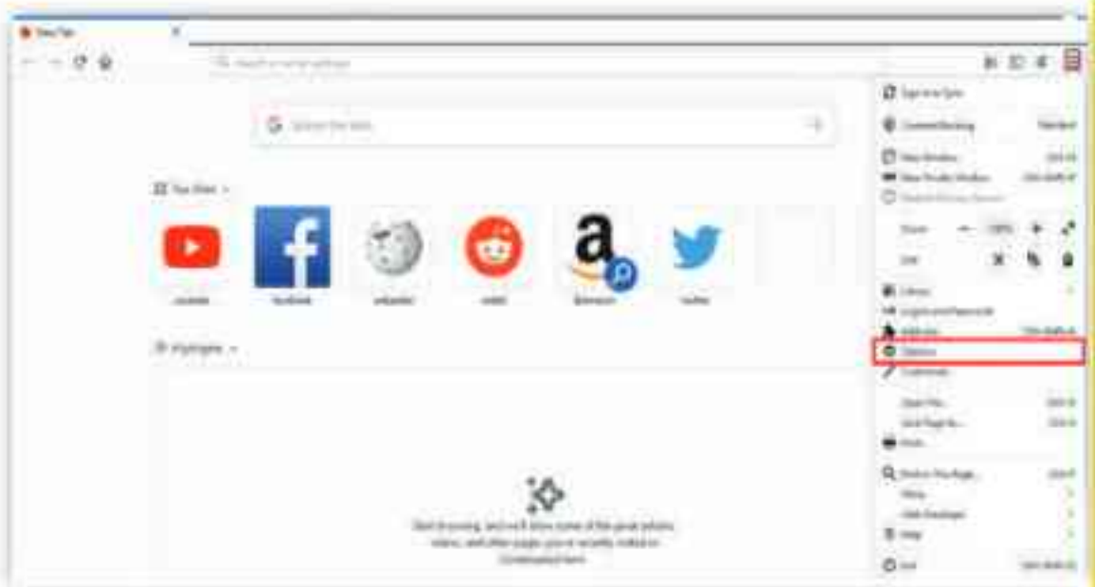
INTERNET EXPLORER



APPLE SAFARI

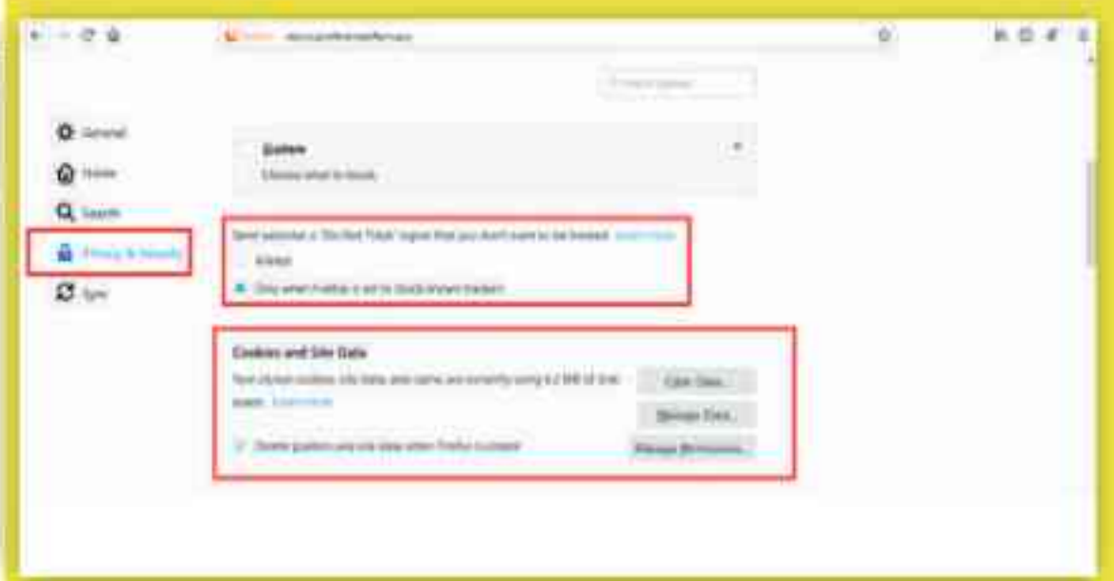


MOZILLA FIREFOX

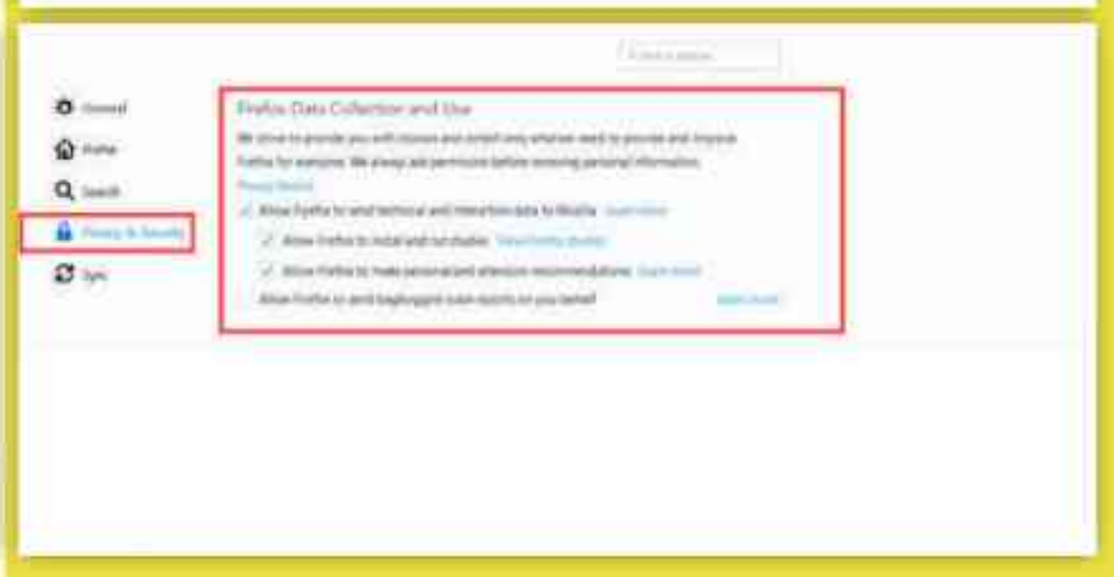






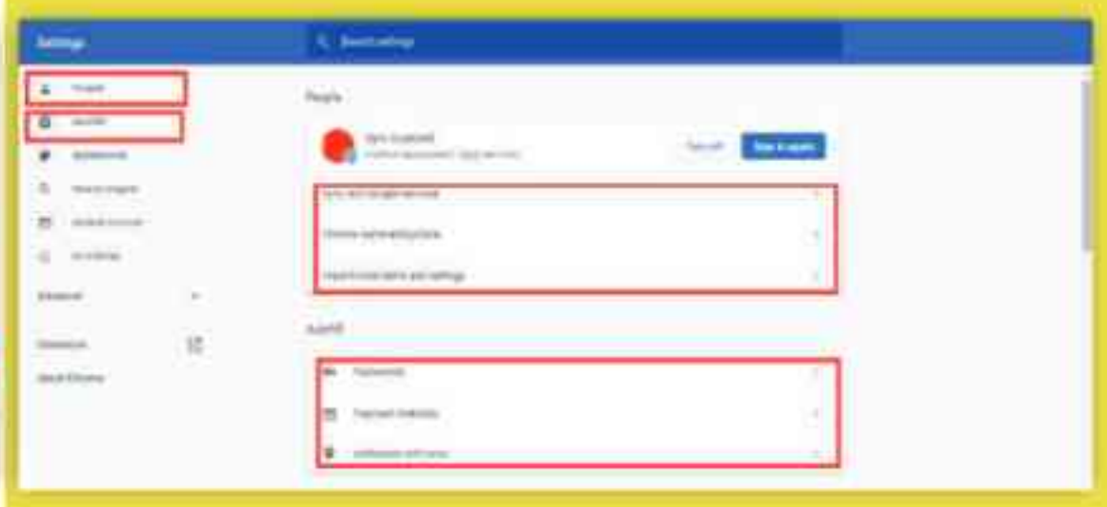


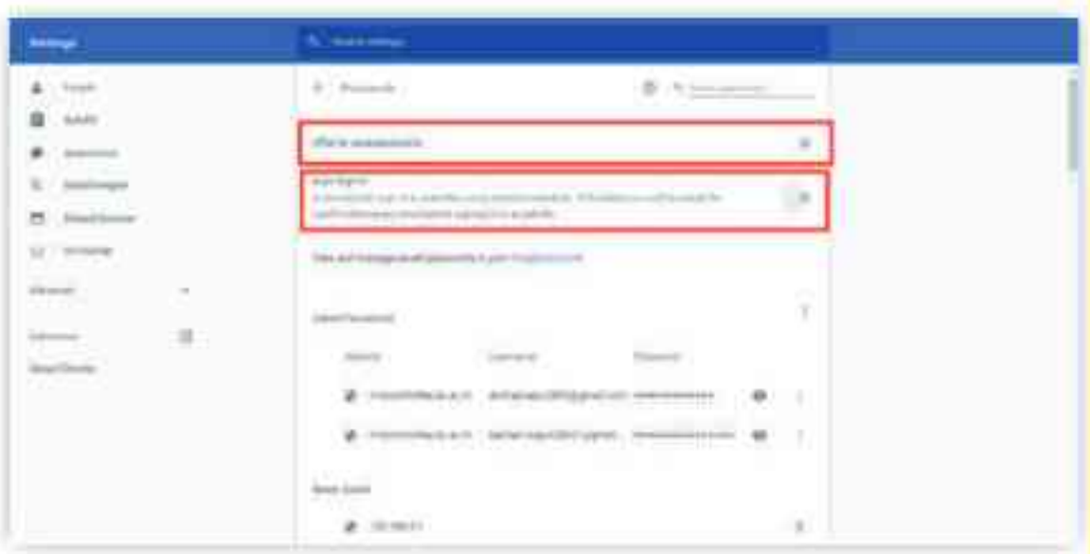


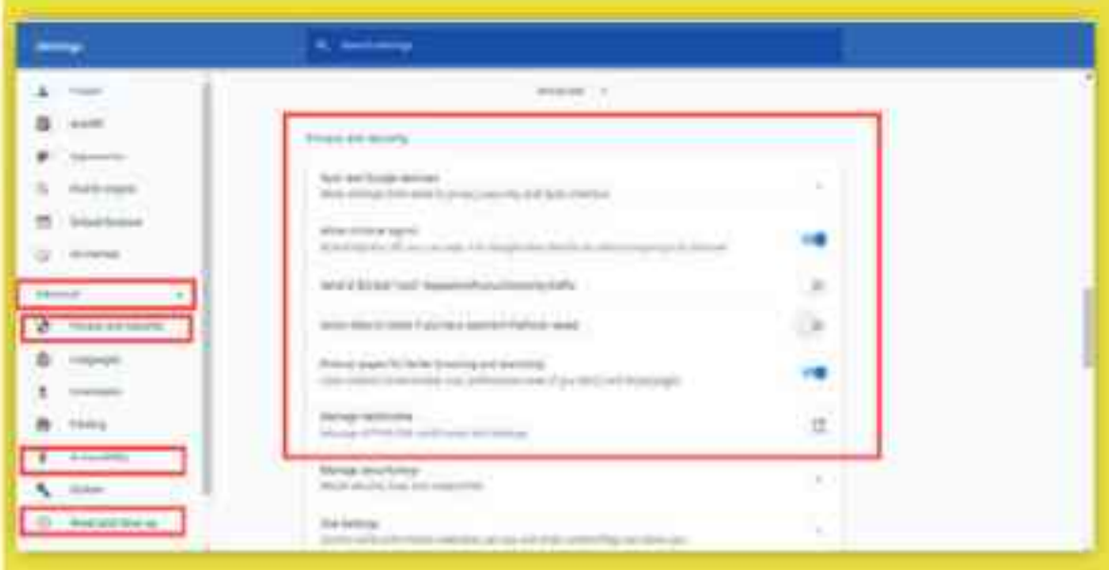


GOOGLE CHROME









Google Chrome

Click on the three vertical dot top right side corner in the Chrome and select Settings. Or simply type ***chrome://settings/*** in the address bar.

People section

Click on Sync and Google services .
Check if the Safe Browsing option, which offers protection from dangerous sites, is enabled.

Autofill section

Click on Passwords and disable Offer to save passwords.
Click Payment methods and disable Save and fill payment methods.
Click on Addresses and more and disable Save and fill addresses.

Advanced Section

In Privacy and security turn off the Allow sites to check if you have payment methods saved.
Click on Site Settings then Cookies and it is recommended to disable Allow sites to save and read cookie data (recommended) and enable Block third-party cookies. Click on Location and make sure that Ask before accessing (recommended) is set or you can block the location access by simply toggling the button.

Click on **Camera** and make sure that **Ask before accessing (recommended)** is set or you can block the camera access by simply toggling the button.

Click on **Microphone** and make sure that **Ask before accessing (recommended)** is set or you can block the microphone access by simply toggling the button.

Click on **Motion sensors** and **Block sites from using motion sensors by simply toggling the button.**

It is highly recommended to disable JavaScript for Security purposes but on disabling JavaScript some webpages may not load properly. To disable **JavaScript** click on JavaScript and then block it.

It also recommended to turn off Flash in Chrome. To check it click on **Flash** and make sure it showing **Block sites from running Flash (recommended).**

Click on **Pop-ups and redirects** and make sure it is Blocked, if not block it.

Click on **Ads** check it is showing **Blocked on sites that show intrusive or misleading ads (recommended).**

Click on **Clipboard** and make sure **Ask when a site wants to see text and images copied to the clipboard (recommended)** is checked.

Make sure your Safari is up-to-date to the latest version. To check for updates just go to the Apple menu and click on Software Update.

Now it's time to secure Safari Preferences. Just go to the Safari Menu and click on Preferences.

In General section uncheck Open "safe" files after downloading.

Select Remove history items as After one day.

In the AutoFill section uncheck the AutoFill web forms options.

On the Passwords section and remove any stored passwords.

In the Security section Check Fraudulent sites option.

In the Web content check Block pop-up windows.

It is recommended to disable JavaScript for security, but some sites may not load properly.

In the bInternet plug-ins uncheck Allow Java and also uncheck Allow all other plug-ins.

In the Privacy section– Select Block cookies as From third parties and advertisers.

Select Limit website access to location as Deny without prompting.

Apple Safari

First of all, click on the Tools icon in the top right corner in Internet Explorer and click **Internet options.**
First of all it is recommended to Update Your Windows to necessary security patches.

In **General** section:

→ It is recommended to change the Home page first. Change it to something reputed search engine.

→ Check the Delete browsing history on exit.

In **Medium-high** section:

→ Set the Security level to High or at least Medium-high.

→ Check the box Enable Protected Mode.

→ Click on Apply.

In **Privacy** Section:

→ Set the Settings to High or at least Medium High.

→ Check the boxNever allow websites to request your physical location.

→ Check Turn on Pop-up Blocker.

→ Check the box forDisable toolbars and extensions when InPrivate Browsing starts.

→ Click onApply.

Internet Explorer

Internet Explorer

In **Connection** Section:

- → Click on settings under theAutoComplete.
- → Uncheck Box for Forms and also for User names and passwords on forms.
- → Check Ask me before saving passwords.

In **Advanced** Section:

Go for the **Security** section and select **Check for publisher's certificate revocation.**

Select **Check for server certificate revocation.**

Select **Check for signatures on downloaded programs.**

Enable **Integrated Windows Authentication.**

Enable native **XMLHTTP support.**

Check the box of **Use SSL 2.0.**

Check the box **Use SSL 3.0.**

Check the box for **Use SSL 1.0.**

Click on **Apply** .

Click on **Ok.**

Finally **restart** the Browser.

Mozilla Firefo

To harden firefox security go fore the **three vertical lines** located in the top right corner in Firefox browser and select Options.

OR, Just type **about: preferences** in the browser address bar also.

First thing Keep your Firefox Up to date for best performance, stability and security and also make sure **Automatically install updates (recommended)** is selected in the **General section.**

In the Search section make sure you have selected a trusted search engine in the **Default Search Engine.**

In the **Content Blocking** area of **Privacy & Security** section make sure the **Standard** protection or **Strict** protection is selected. Strict protection may cause some sites to break but Standard protection will be good enough.

In **Cookies and Site Data** check the option **Delete cookies and site data when Firefox is closed.** It will delete all of your cookies after you close the Firefox browser.

Check the **Ask to save logins and passwords** for websites option in the Login and Passwords area.

Check **Use a master password.** It will pop up a window where you can set a master password. A master Password is used to protect sensitive information like site password. If you create a Master Password you will be asked to enter it once per session when Firefox retrieves saved information protected by the password.

In **History** select **Use custom settings for history** and uncheck **Remember browsing and download history** and **Remember search and form history** and also check **Clear history when Firefox closes.**

In **Permissions** Click the **Settings** right beside **Location** and add the trusted sites which can access the Location.

Click the **Settings** right beside **Camera** and add the trusted sites which can access the **Camera.**

Click the **Settings** right beside **Microphone** and add the trusted sites which can access the **Microphone.**

Check **Block websites from automatically playing sound** and also you can set exception for the sites which trust.

Check **Block pop-up windows** and also you can set exception for the sites which trust.

Check **Warn you when websites try to install add-ons** to prevent anty third party website to install add-ons in the browser.

In the **Firefox Data Collection and Use** uncheck **Allow Firefox to send technical and interaction data to Mozilla.**

Uncheck **Allow Firefox to make personalized extension recommendations.**

Uncheck **Allow Firefox to send backlogged crash reports on your behalf.**

In the **Security** make sure that **Block dangerous and deceptive content** is checked.

Check **Block dangerous downloads** option.

Check **Warn you about unwanted and uncommon software.**

Select **Ask you every time** when a server requests your personal certificate.

Check **Query OCSP responder servers to confirm the current validity of certificates.**

Always install Plugins and Extensions from official Mozilla foundation. To install add-ons in Firefox go to Add-ons by going that three vertical lines mentioned earlier and install as per your requirements.

Mozilla Firefox



https://www.youtube.com/watch?v=uoMfcvDxlKQ

WATCH

8.3.4 Beware Of Strangers And Suspicious Links

Taking regular data backups is an important strategy for securing all your important data. A backup is the only way to restore the original data.

Why you must have Data Backup

Data on a hard disk can be lost for a variety of reasons, such as:-

- Hardware failure;
- Operating system failure, e.g., file system crash.
-Files or volumes modified or deleted accidentally by yourself.
-Files or volumes modified or deleted intentionally by intruder.
-Files or volumes modified or deleted by virus or malicious codes.

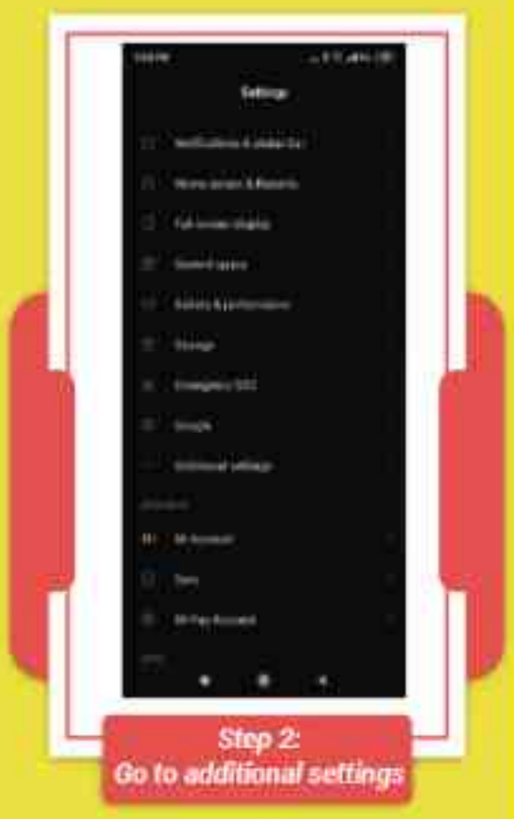


Back Ups

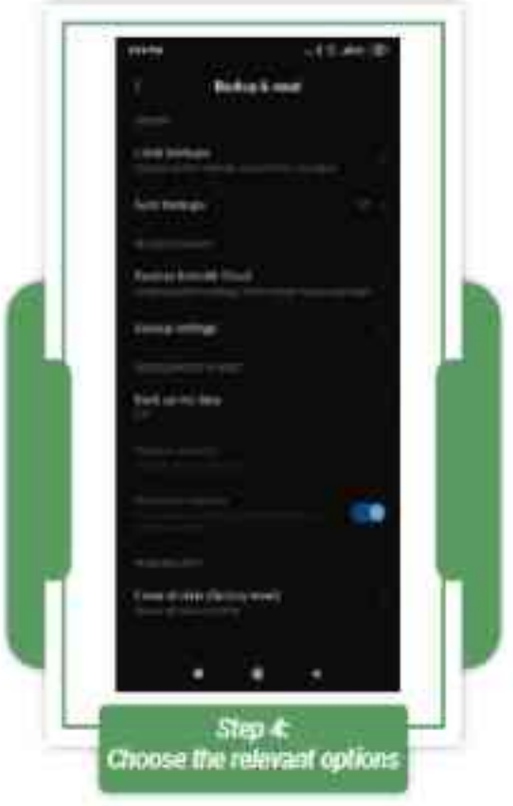
You can also take a backup of your data to keep it safe.
Many companies like Apple, Xiaomi, Samsung have inbuilt backup features in their phones.

You Can Find The Option In The Settings, As Shown Below.

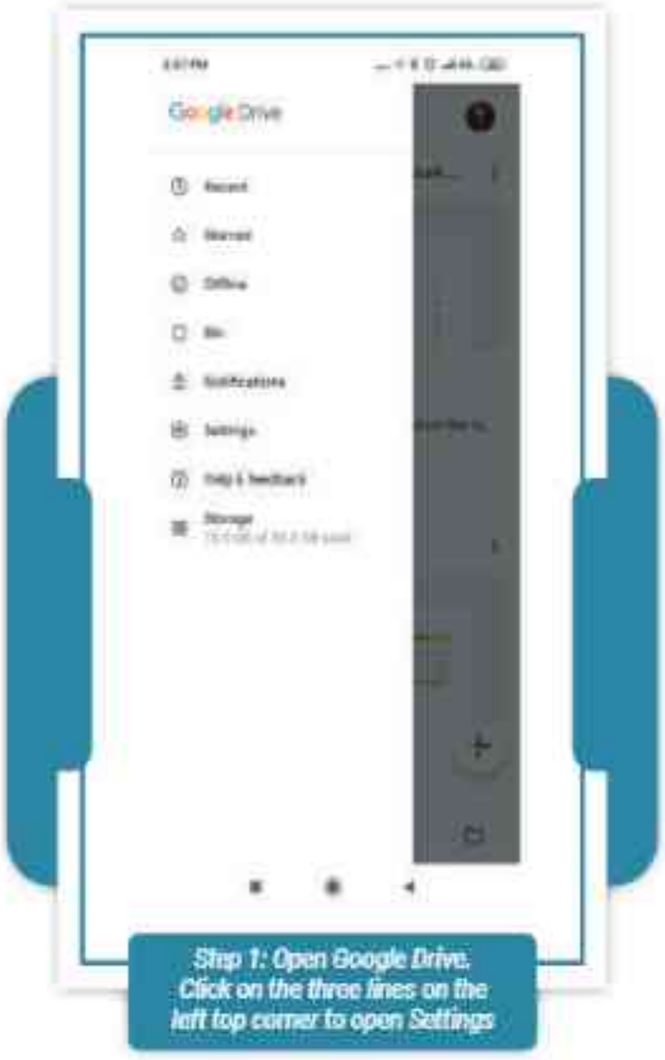




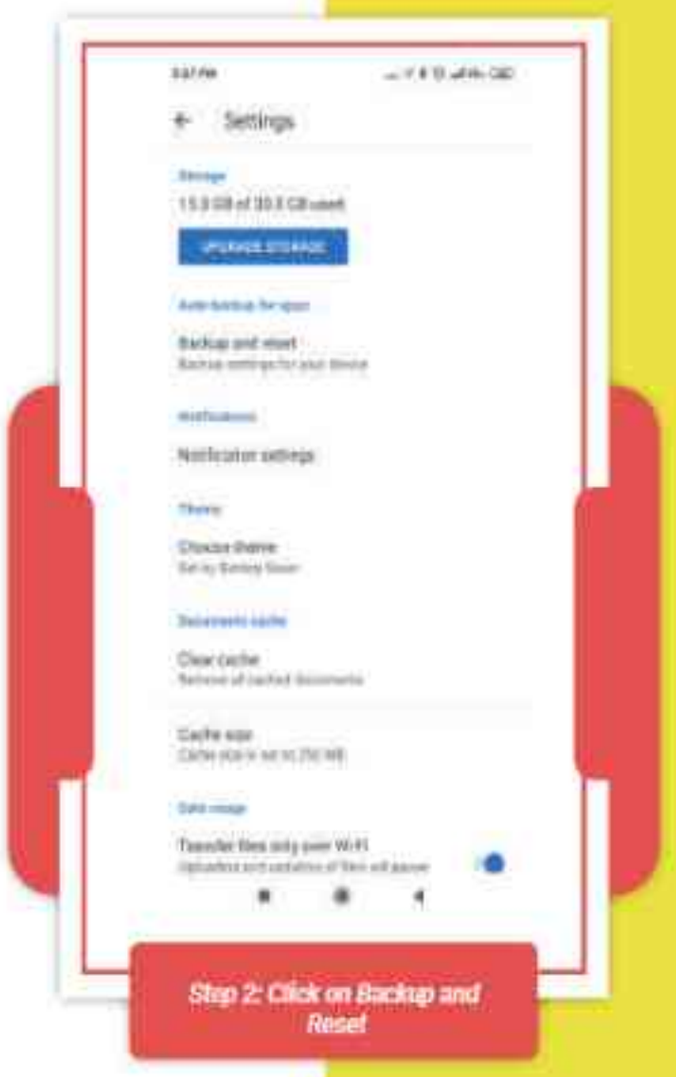




You Can Also Use Google Drive To Take A Backup Of Your Data.



Step 1: Open Google Drive. Click on the three lines on the left top corner to open Settings

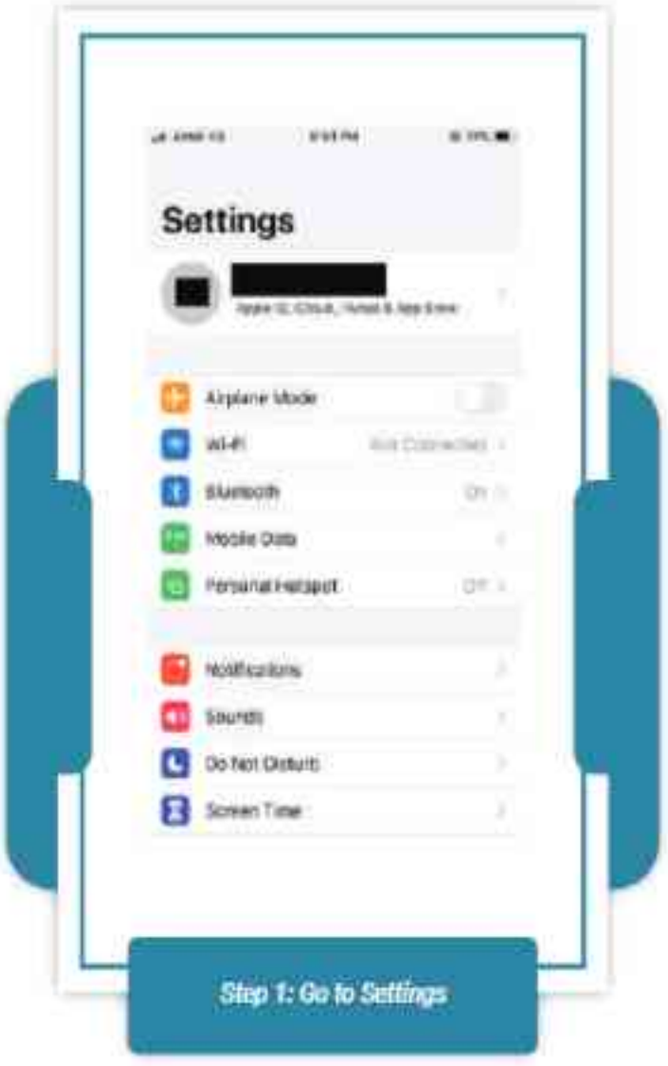


Step 2: Click on Backup and Reset

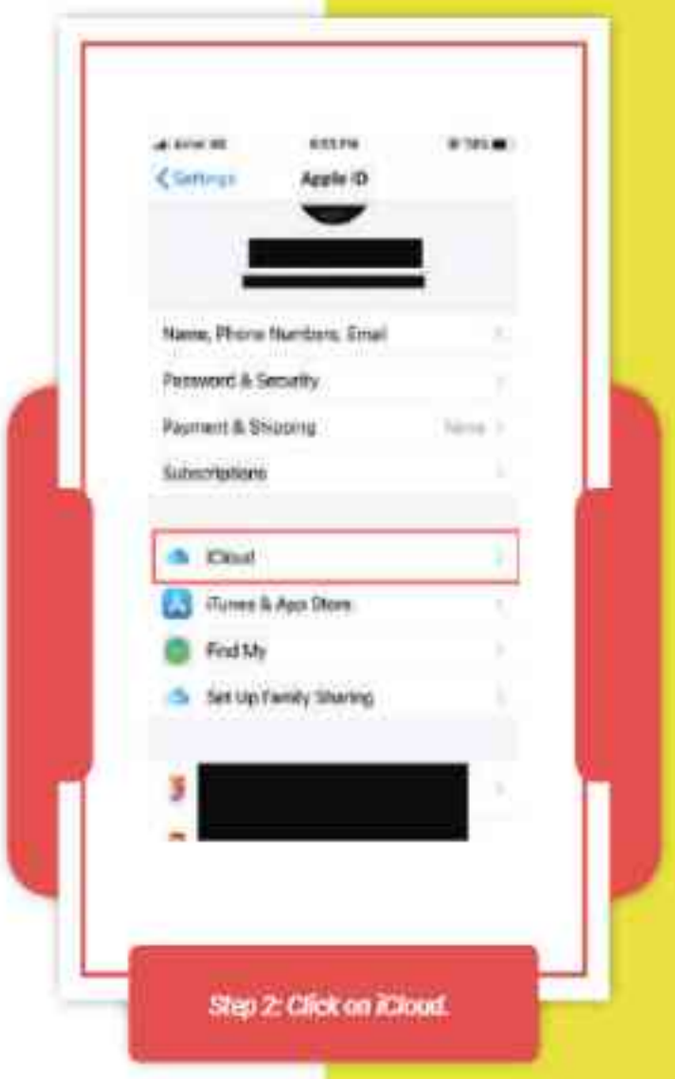


Step 3: Turn on the option. Your data will now be stored on Google drive as well.

Backup On iPhones



Step 1: Go to Settings



Step 2: Click on iCloud.



Step 3: Take backup of all the applications that you wish to.



https://www.youtube.com/watch?v=RGJ1oiNOxBI

WATCH

8.4 PERSONAL SECURITY

If you wouldn't accept this offline, why would you accept this behaviour online?

If there are people offline who you would be uncomfortable talking to about your physical / sexual experiences, chances are, you'd be uncomfortable doing this with strangers online too. Cyber Groomers who create fake accounts to befriend people, for the purpose of harming them whether physically, sexually or emotionally.

What you CAN DO with continued harassment:

a) Coming across cyber groomers, your first instinct should be to block and report them on the platform.

b) Don't stay silent, speak to someone you trust who will be able to help. It can be a parent, a teacher, a friend, anyone who you think can give you the support you need to see it through that you are no longer affected by the cyber attacker online. If they're digitally savvy, they'll help you implement security measures to stay safe online!



Be cautious when your chat partner gives you many compliments regarding your appearance within a short span of your acquaintance.

Do not talk to people who ask you to share your sexually explicit photographs or videos. Never accept a friend request from someone you have never met in person. If you share your sexually explicit photos or videos with someone, the person can share those photos with others or post them on social media. They can also blackmail you.

This point was made previously, but we stress it: never turn on your webcam if your chat partner does not connect to the webcam. Keep your webcam private. Put a sticker over your webcam, laptop camera, or phone camera when they aren't in use. These devices can sometimes be hacked and used to take pictures or videos of you without your consent.

People are not always who they say they are. Learn more about protecting yourself when using social media. You should be very careful in the chat rooms. Never share personal details and limit your identity.

a) Protect your online reputation: Use the services provided to manage your digital footprints and 'think before you post'. Even if offensive posts and pictures are removed by appealing to the service providers, the possibility of someone taking screenshots or downloading the content cannot be ruled out.

b) Do not go to meet a person whom you met online alone.





8.4.1 Abide By The Law

Use reliable services and know how to legally access the music, film and TV you want.

Acknowledge your sources: use trustworthy content and remember to give credit when using others' work/ideas. Think about something you have worked hard for, and imagine that someone online would want to receive the same consideration and receive credit for their work.

8.4.2 Seek Help

Know where to find help: Understand how to report to service providers and use blocking and deleting tools. If something happens that upsets you online, it is never too late to tell someone.

Talk to your elders or parents, if your chat partner suggests to keep your conversation with them a secret. You can also report these to Childline at 1098.



You can protect yourself from becoming a victim of grooming:

a) Take all precautions about sharing personal information and identity details during chats or in public spaces.

b) If groomer is using social media platforms to groom you, you can block him/her. All the social media apps or services have the option to block a user.

c) Save messages, pictures or videos shared with you by the groomer. Such messages, pictures or videos can be used as an evidence to initiate legal action.

d) Your parents/elders can contact local police station to lodge a complaint against the groomer.

Do check with your parents before downloading apps or sharing personal information.

This is mandatory for anyone below the age of 14. Some apps are malicious in nature. Therefore, to prevent malpractices, it is important to share the information with parents.

Also, Facebook policy does not allow any student below the age of 14 to use the app. Even Netflix, YouTube and Amazon Prime mandates 'Kids mode' for all children below the age of 14.

Dealing With Unauthorized Access

Giving Permissions to apps: While installing apps, give only those permissions that are absolutely essential for the functioning of the apps. Of any application does not function without all permissions, it is best to not install it.

Sharing the device's location: Always allow those app with device location permission which actually required.

Via GPS:

Via Geotagging: Link your location with your posts, only when you are sharing it with people that you know and trust. sharing your location with strangers or merely making it public may compromise your security.

Certain characteristics of the digital environment magnify the risk that children will be exploited or abused by other users. In particular, online abusers can easily operate anonymously and bypass gatekeepers such as parents or teachers. When children are bullied online, such as through 'revenge porn', their humiliation can be very public.

Online grooming: deceiving a child for sexual purposes – is on the rise, although its extent remains unknown. The sexual abuse that follows may be online, such as by 'sexting' – sending or eliciting explicit sexual images – or offline, if the victim is lured into a meeting.

Cyber-bullying which takes several forms is becoming more common and can have a profound impact on mental health, well-being, and educational attainment. When children go online they are more likely to bully others, and to be bullied, than when they are offline.

Consent Empower children to decide for themselves how others collect and use their information by requiring their consent. As of now, there is no minimum age of digital consent in India.





ACTIVITY 1

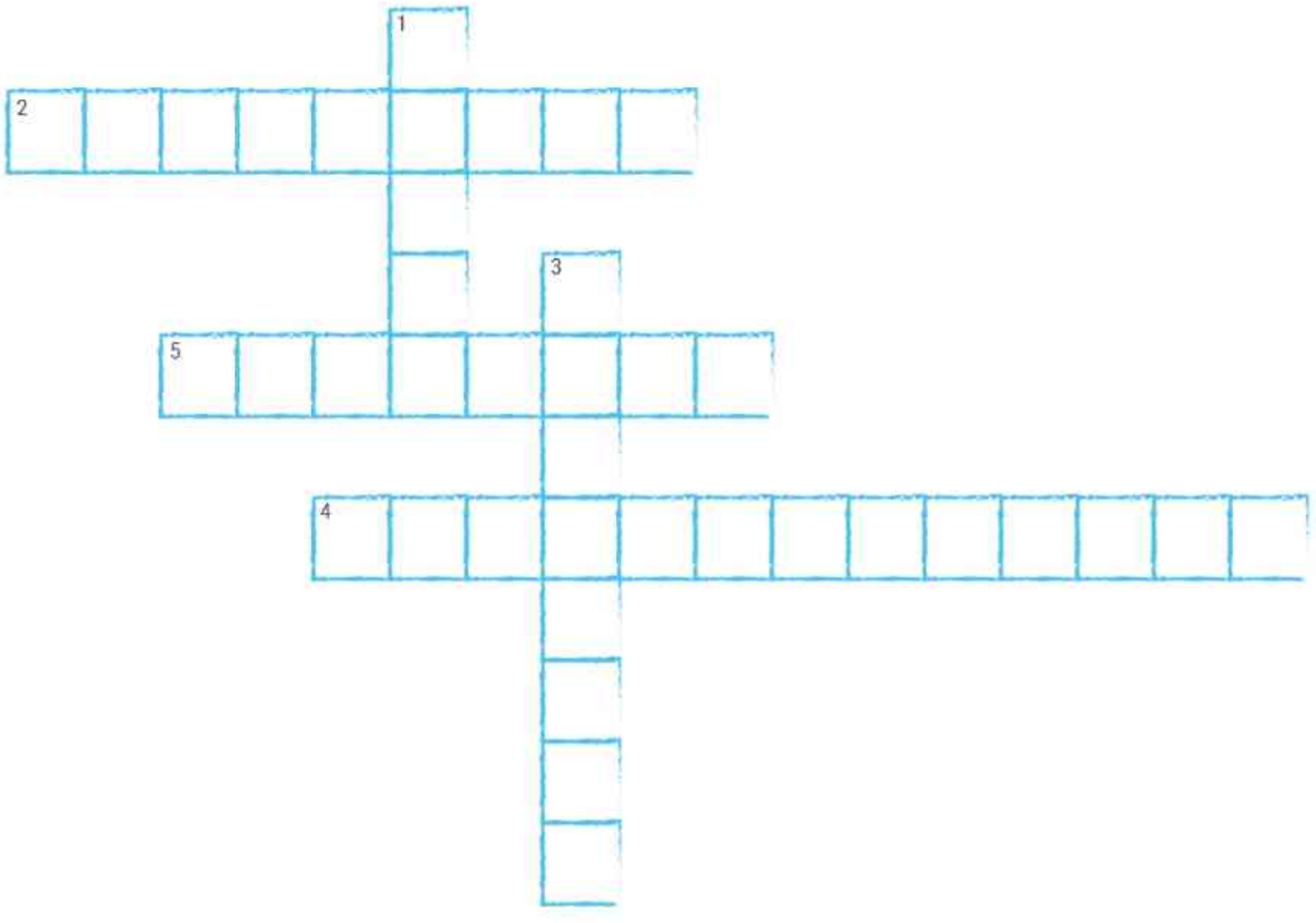
Internet safety crossword.

DOWN

1. Software programs designed to corrupt computers
3. Software protecting incoming and outgoing network connections from unwanted access

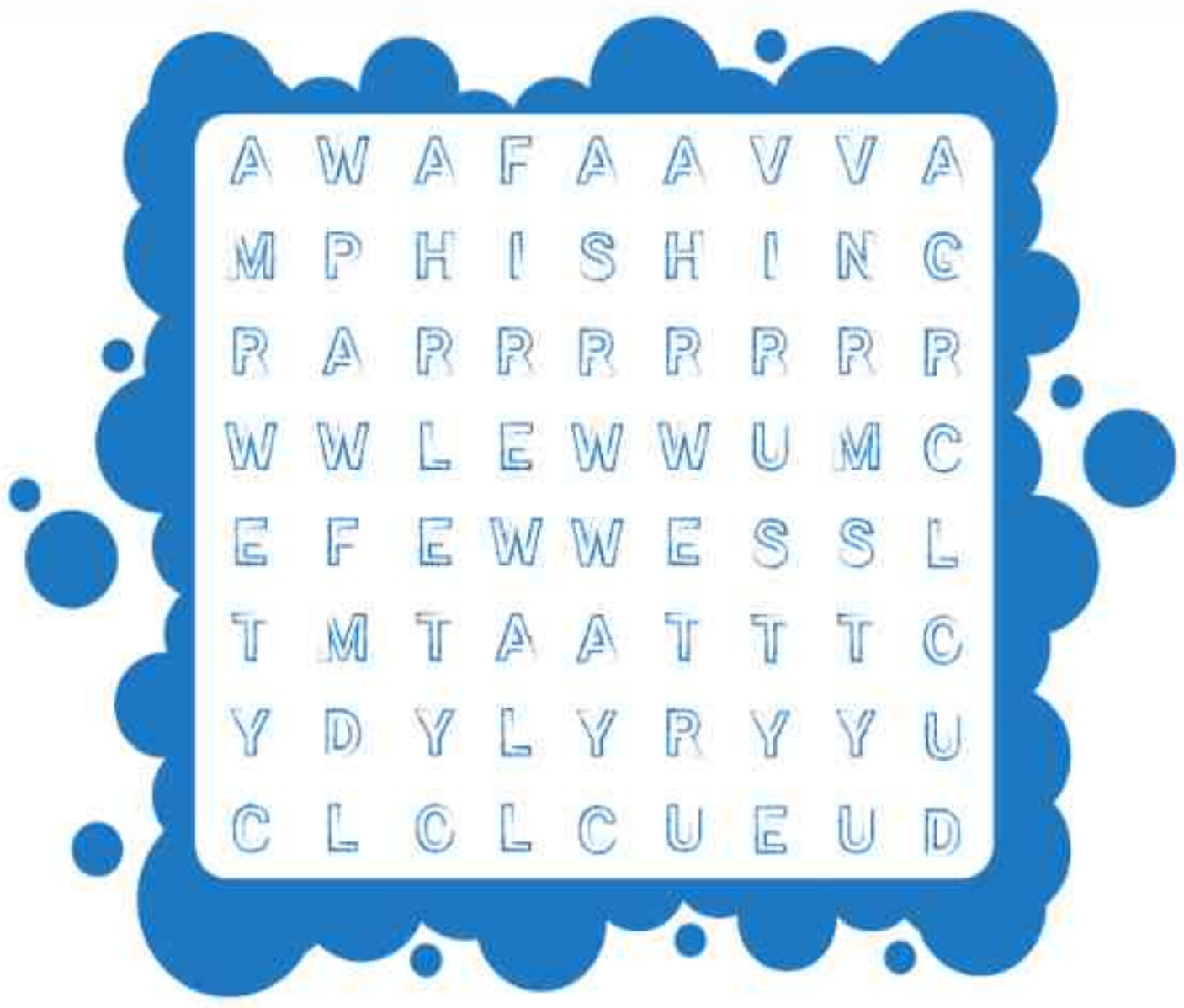
ACROSS

2. Protection for your computer
4. Being troubled or embarrassed online
5. Trying to steal other people's sensitive information



ACTIVITY 2

Word search:
Find the maximum number of words related to cyber security.



ACTIVITY 3

Multiple choice questions (✓)

1. **Which of the following do you think is a strong password?**
   - ○ An$#yOuM@n!071
   - ○ 9570000066@pass
   - ○ Loveyou3000
   - ○ All of the above

2. **Which of the below mentioned links are suspicious?**
   - ○ https://www.faceb00k.com
   - ○ http://www.amazone.com
   - ○ htps:/www.google.com
   - ○ All of the above

ACTIVITY 4

List three ways by which you protect yourself from threats and risks on digital devices.

01

02

03

ACTIVITY 5

What is stalkerware?



09 DIGITAL LAW

9.1 WHAT IS DIGITAL LAW?

Digital law can be defined as the legal rights and restrictions governing technology use. Most users are unaware of the possible consequences of their online activities thereby need to be made aware of the rules and legal implications of using the internet.

The following are some actions that are unethical or illegal:

a) Software or systems piracy.

b) Downloading music and films without authorisation or payment.

c) Stealing other people's work (plagiarism and copyright infringement), personal data (identity theft) .

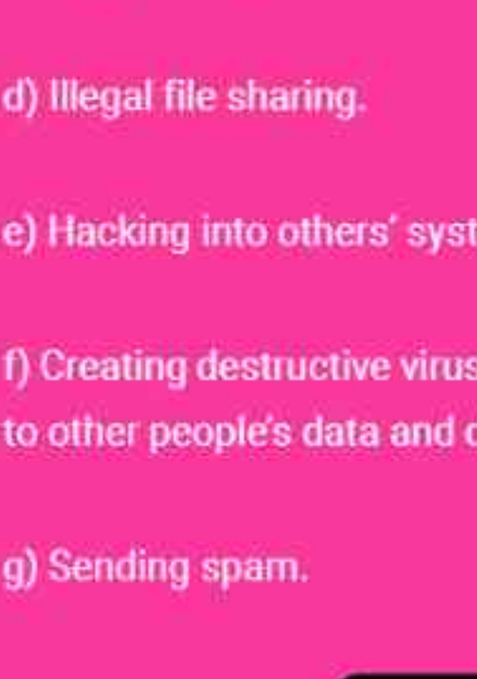
d) Illegal file sharing.

e) Hacking into others' systems or networks.

f) Creating destructive viruses or worms that causes damage to other people's data and devices.

g) Sending spam.

- Think before you act. You may be violating the law of the land.
- Ignorance of the law is not a valid defence in legal fora.
- What is ethical is generally legal.



9.2 ILLEGAL ACTIVITIES USING DIGITAL TECHNOLOGIES

Plagiarism is an act of using or closely rewording the language and thoughts of another author without seeking their permission or representing another author's work as yours without giving credit to the author. Stealing other people's work in the form of words, ideas, images or data with permission is both illegal and unethical. When using online resources for school projects, assignments, essays, give credit or acknowledge the author(s) of the resource.
Copyright infringement: Involves using someone else's work but not paying them for it. For example, using a photograph found online without seeking the photographer's permission or not paying for using it is a copyright violation.

Plagiarism can affect academic and professional reputations while copyright infringement is a violation of the law and penalties can be imposed.

Fair use is an exception to the restrictions imposed by copyright law. Quoting a few lines from a copyrighted work in an academic paper with proper citation generally qualifies as "fair use".

Do remember

- The purpose of the work should be academic, not-for-profit, and educational.
- The piece is not copied in its entirety. A few lines from the original are quoted.
- The reference does not have any impact on the value of the original work.

9.2.1 Sexting

Sexting is sharing of sexually explicit texts, photos or videos of naked or semi-naked pictures of themselves or others through mobile or social media platforms.
The growing number of such reported cases of sexting and self-exposure highlight the vulnerability of children and young people to blackmail and extortion (including "sextortion") and "revenge porn".
Victimizing by way of revenge porn is often practiced by children below 18 years of age. It may be described as "an act whereby a perpetrator satisfies his anger and frustration for a

broken relationship through publicizing false, sexually provocative portrayal of his/her victim, by misusing information that he may have known naturally and that he may have stored on his computer, or phone, or may have been conveyed to his electronic device by the victim herself, or may have been stored in the device with the consent of the victim herself; and which may essentially have been done to publicly defame the victim.

9.2.2 Online Child Abuse And Exploitation

There is global consensus that child sexual abuse and exploitation is unacceptable offline or online. Under no circumstances is the production, distribution and viewership of sexually explicit images of children is permitted. The law imposes strict penalty and punishment on anyone found to be taking, sharing and viewing such pictures.

9.2.3 Defamation

Social media, email groups, bulletin boards and other digital spaces enable widespread offensive content against a person to be posted. Offensive messages such as body shaming, name calling on social media especially can be very hurtful. As the messages spread around so quickly it can cause a lot of distress to the person targeted. Although defamation is not a criminal offence it is unethical and should be avoided.



9.3 LEGAL PENALTIES FOR ONLINE OFFENCES

Indian laws deal with many of the core issues related to digital technologies. You need to understand that some of your online actions may be on the borderline of an offence and some may actually be infringing the law.



Being Smart Online Checklists

Checklist: How to keep the devices safe?

I. Be alert

Keep the devices clean

a) Ensure you keep your internet-connected devices, like laptops, phones and tablets, safe from malware.

b) Make sure software of operating systems is up-to-date. Also make sure security software that updates automatically is installed on devices.

II. Keep devices safe

Mobile phones

a) Use a screen lock to lock your smartphone.

b) Protect sensitive data by taking regular backups either on Dropbox, OneDrive or iCloud.

c) Always switch off your wireless connections e.g. Bluetooth,Wi-Fi, NFC, etc. when not in use.

d) Use genuine web browsers and never save your login credentials, banking details.

e) Install an antivirus on your smartphone.

III. Be smart

Manage mobile apps:

a) Keep apps on your mobile devices updated. Updates often have security fixes in them.

b) Delete apps you no longer use. It would also entail clearing of the cache.



Illegal online activity	Laws covering offense	Penalty
Posting or sharing of inappropriate images and comments online or through WhatsApp.	Protection of Children Against Sexual Offences Indian Penal Code, Information Technology Act, 2000.	A term of up to 3-5 years imprisonment and also a fine.
Revenge porn If an inappropriate picture or explicit selfie has been shared by a friend, for taking revenge threatening to circulate this to a wider group or demanding a favour for not doing so.	POCSO, 2012 Indian Penal Code.	A term of up to 7 years imprisonment with a fine In case of extreme effect of the said act like committing suicide or attempt to commit suicide, the punishment may go upto life term as well.
Violation of privacy Uses any electronic device and/or online medium to record, circulate, transmit, publish or bring into the public domain any image, photograph, film, videotape, MMS etc. that has private parts of a child captured in violation of his privacy commits the offence of 'Violation of privacy of a child'.	IT Act 2000 POCSO Act, 2012.	A term of upto 7 years imprisonment or a fine or both.
Impersonation Sending someone messages by assuming a false identity.	Information Technology Act, 2000.	A term of up to 3 years imprisonment and also a fine.
Unauthorised access Hacking someone's computer, email or social networking account.	Information Technology Act, 2000.	A term of up to 2-3 years imprisonment or fine or both.
Online piracy Downloading movies and music for free. Illegally copying or distributing software using the internet without the consent of the rights owner.	Copyright Act, 1957.	Punishment of a term up to 6 months to 3 years of imprisonment and fine.
Plagiarism Using words, ideas, images or data of another person without attributing the source.	Copyright Act, 1957.	A term of imprisonment from 6 months to 3 years and fine.
Misrepresentation Falsification of age for the purpose of creating accounts or accessing certain websites. It amounts to entering under a contract with the service provider based on misrepresentation of facts and real identity.	Indian Contracts Act together with IPC.	A term of imprisonment up to three years, or fine, or both.
Defamation Posting defamatory statements, images or videos, about a person on social media, chats, bulletin boards or any digital space.	Indian Penal Code.	A term of upto 2-3 years imprisonment , or fine, or both.

9.4 GOOD PRACTICES

What you write is clearly your prerogative. But do remember that any production, consumption and distribution of content which involves sexual imagery of children is illegal.

Choose friends wisely. *Everything is not about the number of friends you have. Select your friends wisely as they can access your information. Learn to delete/block unwanted friends.*

Think before saying anything. *Be mindful of what you post/update on Facebook. Ask if you will regret it five years later. Do not become a part of hate-groups.*
Manage privacy settings. Your posts are publicly shared unless you go to settings and change your Security and Privacy to Only Friends.

Keep in mind the dangers of sharing. *Be careful of what information you put out on Facebook. Check your posts and images for indicators of your whereabouts or anything that may invite unwanted users.*

Create friends lists to manage your posts. *Create separate lists for your acquaintances, friends, family etc. This will make it easy to regulate or control who can see your posts.*

Look out for suspicious activities. *Do not click on suspicious links. Beware of fake Facebook pages that steal your password. If your account is hacked, change your password or report to Facebook.*

Consider the whole image. *Ask yourself if the image or the background giving an indication where you were or what you were doing at the time of taking the picture. If yes, then reconsider posting it.*

Manage your visibility. Photos you are tagged in are visible to everyone. To make it secure you can make your account private by going to the menu on the (top right side) on your profile.

Accepting followers. If your account is private you can approve who follows you. Do not accept requests from strangers. Also be mindful of who you are following.

Block/report unwanted contacts. Go to their profile and tap menu (top right side) to report and block. You can also report images by going to menu option at the top of each image.

"Untag" yourself. You can untag yourself by tapping on your username in the post, provided the post is public or you follow the person who tagged you.

Other tips. Switch off geotagging and location feature. Delete your post if you are not sure about it. Posts are easy to embed in other websites. It may go viral.

Being safe on social media platforms

Screen capture is possible even on Snapchat, which does not save images. Screen shots are an easy way to save images, and many third party apps auto-save images.

Notification is not guaranteed. Snapchat tells you when your snap was viewed or screenshot. But this function is not always reliable.

Manage your privacy settings. Tap on the ghost icon on the top of your camera screen-> Settings (gear icon)-> 'who can' section-> change settings from Everyone to My Friends.

Threat of unknown users. Tap and hold the user and select gear icon to Block unwanted users.' Add Nearby' may seem cool but keep in mind it can be risky.

Sexting concern. Avoid sharing snap stories that you do not want others to access. Do not share sexually explicit pictures as these may easily go viral.

Keep your User ID Private. Do not post your username on social media as it may attract unwanted attention. Also do not share your password with anyone.

Other instant messaging applications

Do not open, accept, or download a file in Instant Messenger from someone you do not know or if you do not know what is in the file.

Contact the sender by email, phone, or some other method to confirm that what they sent was not a virus.

Visit Microsoft Update to scan your windows computer and install any high-priority updates that are offered to your PC. If you have Automatic Updates enabled, you have to make sure you install them when received.

Use up-to-date version of your Instant Messenger software for better protection of your computer against viruses and spyware.

Upgrade from MSN Messenger to Windows Live Messenger in order to block attachments that may contain malware and allow scanning of attachments for viruses.

"Spim" (a short form of spam over instant messaging) uses IM platforms to send spam messages over IM. Like email spam messages, a spim message may contain advertisements or weblinks, by clicking on those links malicious code enters into your PC.

Anti-spyware software can protects the digital device and helps in removing any spyware you may already have. Windows Defender may be downloaded in the absence of anti-spyware software.

Source: www.aarambhindia.org; https://infose-cawareness.in/home/index.php

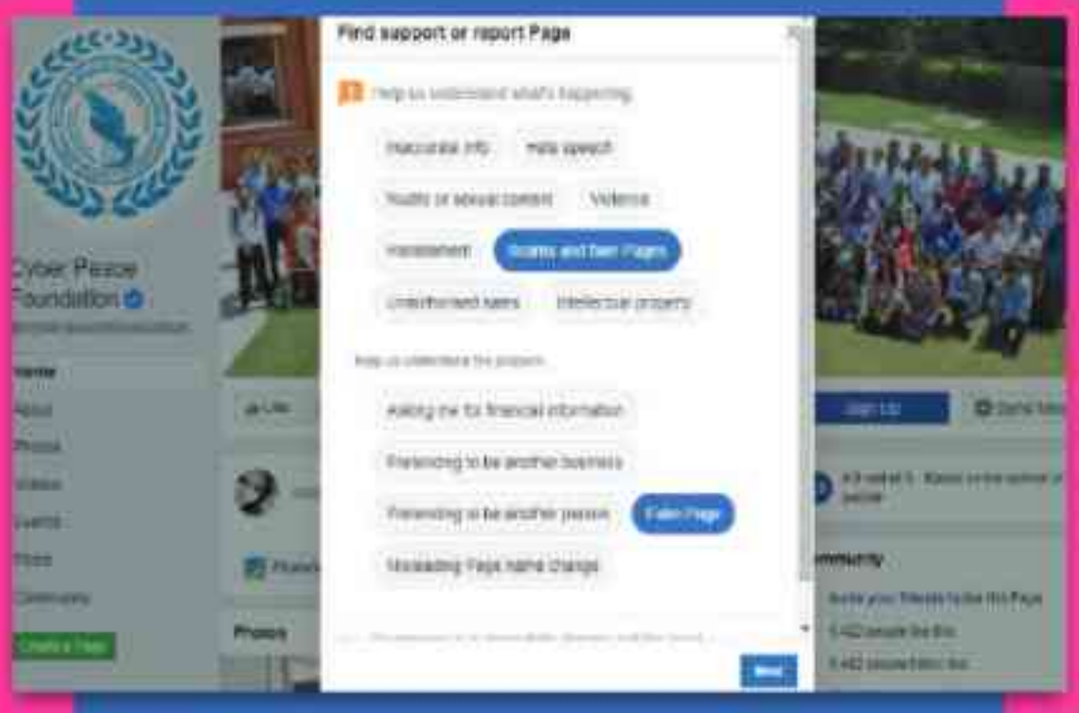
9.5 AVAILABLE REDRESSAL MECHANISMS

9.5.1 Social Media Platforms

Step 1: *If you wish to report any account/post/comment, go to the 3 dots on the right top corner of the account/post/comment. When you click on the dots, you will find the option "Give Feedback or Report". Click on it.*



Step 2: *You will be presented with a list of reasons to ascertain why you wish to report that content.*



Step 3: *Choose the appropriate reason and click on "Done".*

Facebook will remove the account/post/comment if it violates the community guidelines of the platform.





Step 1: If you come across any content that you wish to report, or get removed, go to the top right corner of the post and you will find three dots.



Step 2: When you click on the dots, you will find the option to "Report".



Step 3: Choose "Spam" of you are reporting commercial content (like advertisments), if what you are reporting is not an ad, choose "It's inappropriate".



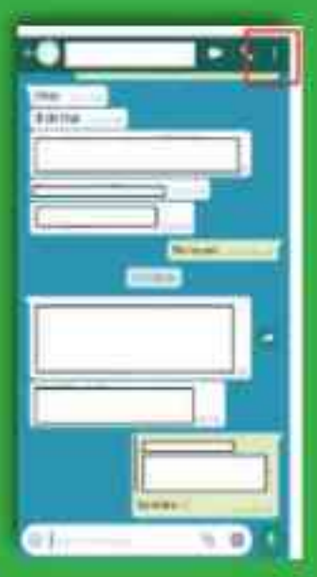
Step 4: Once you click on "Report", you will be presented with a list of reasons to ascertain why you wish to report that content.



Step 5: Choose the appropriate reason and click on "Next".

Instagram will remove the content if it violates the community guidelines of the platform.





Step 1: If you wish to report any number on WhatsApp, go to the 3 dots on the right-top corner of the chat.



Step 2: When you click on the dots, you will find the option "More". Click on it.



Step 3: You will then see the option to "Report". Click on it.



Step 4: You can block the person as well when you report their account. Once reported the account may be deleted if it violates the community guidelines of the platform.



Step 1: If you wish to report any comment you see on YouTube, go to the comment section.



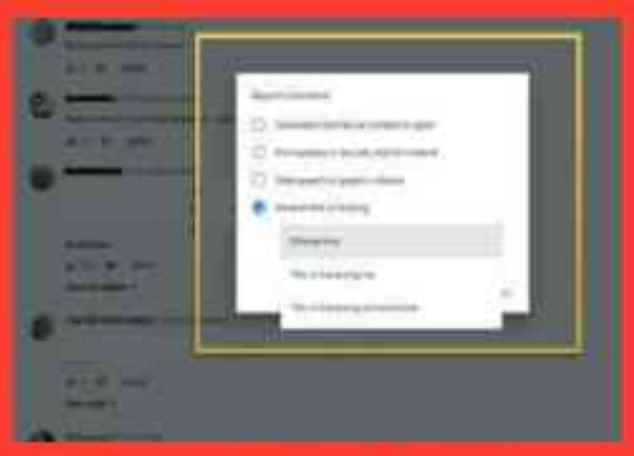
Step 2: Next to the comment you wish to report, you will find 3 dots on the right top corner.



Step 3: When you click on the dots, you will find the option to "Report"



Step 4: Once you click on "Report", you will be presented with a list of reasons to ascertain why you wish to report that content.



Step 5: Choose the appropriate reason and click on "Done".



YouTube will remove the content if it violates the community guidelines of the platform.

Social media platforms have similar processes for reporting objectionable photos, videos, accounts and comments or any other content. Click on the three dots on the corner of the post to go to the "report" option. Report objectionable content by choosing the appropriate reason.

Twitter:
https://help.twitter.com/en/contact-us

For Facebook:
https://m.facebook.com/help/

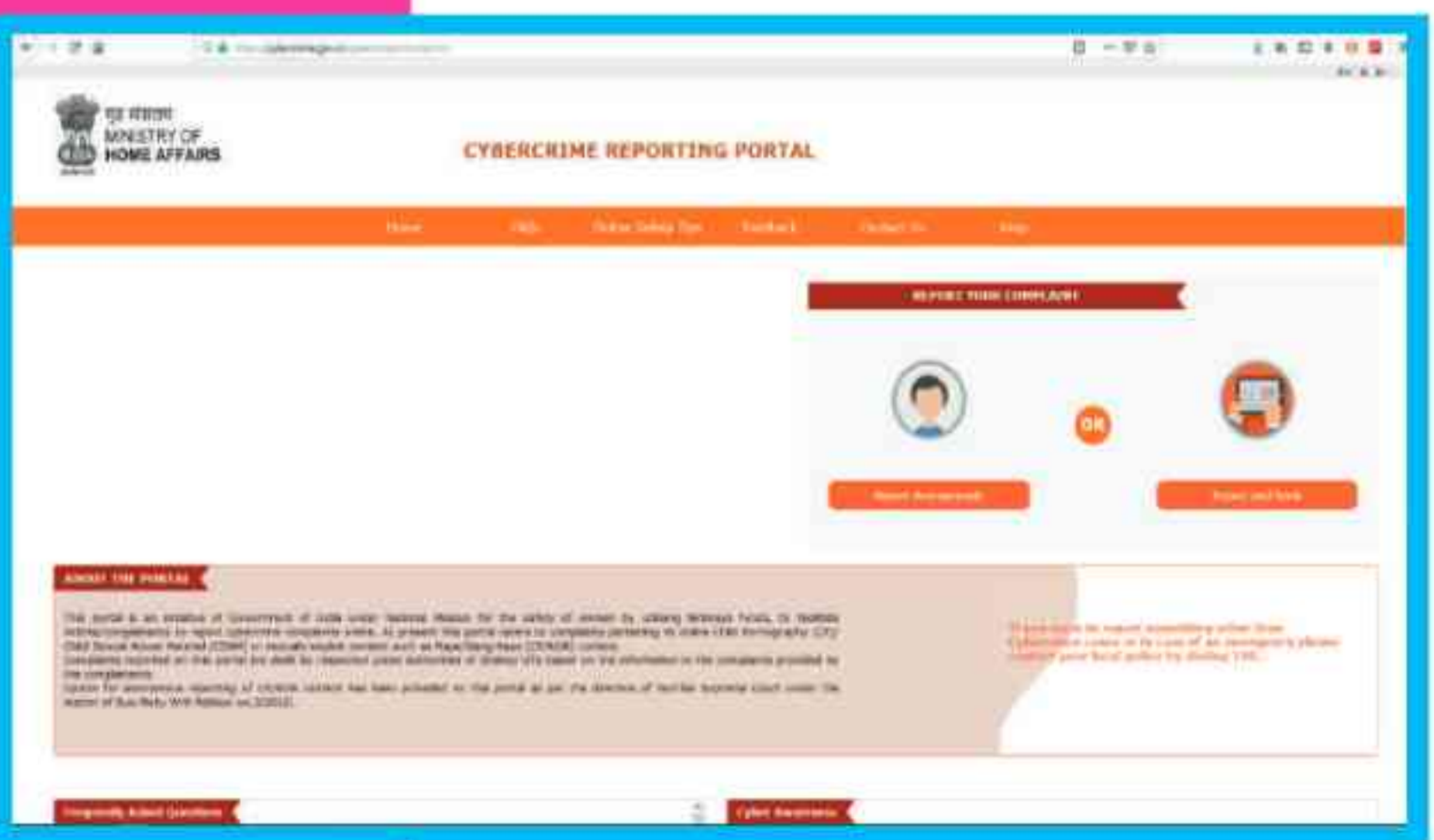
Instagram:
https://help.instagram.com/

Youtube:
https://www.youtube.com/t/contact_us

9.5.2 Police

Reporting on cybercrime.gov.in

Portal run and maintained by Ministry of Home Affairs, Government of India



Log into the cybercrime portal of the Ministry of Home Affairs ***www.cybercrime.gov.in***

The Ministry of Home Affairs, Government of India, has set up a portal to facilitate online complaints of cybercrimes, including online child pornography, child sexual abuse materials, and sexually explicit content (e.g., sexual harassment, abuse, rape and gang rape). Police authorities of relevant states and union territories initiate investigations and legal processes based on the information provided by the complainants. The portal also has the option for anonymous reporting of child pornography and sexually explicit content.



Reporting to the police cyber cell

Children, parents or other concerned adults on their behalf, can approach the cyber cells of the State police to report any online offence. Unlike other crimes, cyber-crimes are not limited by jurisdiction. You can report to the cyber-cell of any city, even if the offense was committed when you were in a different city.

Filing an FIR with the local police

In case you are unable to file a complaint in the cyber cell, you can file an FIR with the local police station. It is not necessary to know the name of the person responsible for the crime to lodge an FIR. Tell the police whatever you know. The local police is expected to coordinate with the cyber cell in the investigation and legal processes.



9.5.3 Childline 1098

CHILDLINE 1098 is India's first 24-hour, free, emergency phone service for children in need of aid and assistance. A child or any adult on his or her behalf can dial 1098, the toll free number to seek help for emergency needs and to avail of long-term care and rehabilitation services.

9.5.4 Ncpcr

Log into the POCSO E-box .

The National Commission for the Protection of Child Rights (NCPCR) set up this online portal to receive complaints regarding sexual abuse and related offences. A child or an adult on his or her behalf can locate the POCSO e-box at the NCPCR site.

http://www.ncpcr.gov or http://www.ncpcr.gov.in/index2.php. It will navigate to a page with the window having a short animation film.





9.6 REPORTING

- Social- Talk to parents, teachers , counsellors .
- Legal- Approach the police.
- Platform - in app reporting, as discussed above.

Content Removal from Websites

If ever any photo or video of yours (that you clicked or appear in), is shared online onto a website without your consent, it can be removed by following the process given below:

1. Find the relevant page or email address for initiating the DMCA request. For example: Search 'Platform/Service name' DMCA on Google. (For eg. Search for "FacebookDMCA" on Google).

2. Carefully open the links suggested on the search page and find either the email address or a form that can be filled.

3. Complete the form to send a DMCA takedown request.

4. If you find an email address, (like contact@abc.com, abuse@abc.com), send an email with Subject 'DMCA Takedown Request' and write clearly about the content and its location (URL or the link to the photo/video) on the platform that you want to remove.



https://www.youtube.com/watch?v=YuTiFfV1gdg&feature=youtu.be

WATCH

Aarambh India

Infosec Awareness, CDAC, MEITY

ACTIVITY 1

Which of the following is illegal? If illegal, what is the penalty?

01 **Plagiarism:**

02 **Impersonation:**

03 **Revenge Porn:**

04 **Unauthorised access:**

05 **Defamation:**

ACTIVITY 2

What are the good practices that should be followed on social media platforms for personal safety and digital security?

ACTIVITY 3

What is the process for lodging a complaint if a cybercrime is committed?



ANSWERS

DIGITAL ACCESS

- **ACTIVITY 1**

(i) (b) Bccnucz (-2 series).
(ii) (a) Tenkrad (1st to last switch).
(iii) (c) GYNX (+5 series).
(iv) (d) Azsfr (-1, +1 series).
(v) (d) Emikof (Replacing vowels with vowels and -1 for constant).

- **ACTIVITY 2**

In a debate, take a stance for or against the motion and frame your arguments on the basis of your research.

DIGITAL LITERACY

- **ACTIVITY 1**

1. False.

The domain names say a lot about websites, .com, .edu, and .gov are among the most credible domain endings for websites. Other variations are much less credible. If any of those three options end a URL, it indicates the website's credibility).

2. False.

When reading online, the resource opens quickly but the pages open one at a time. There may be some brief load times when flipping pages. But when reading offline, the resources may take several seconds to open as the entire file is decrypted.

3. True.

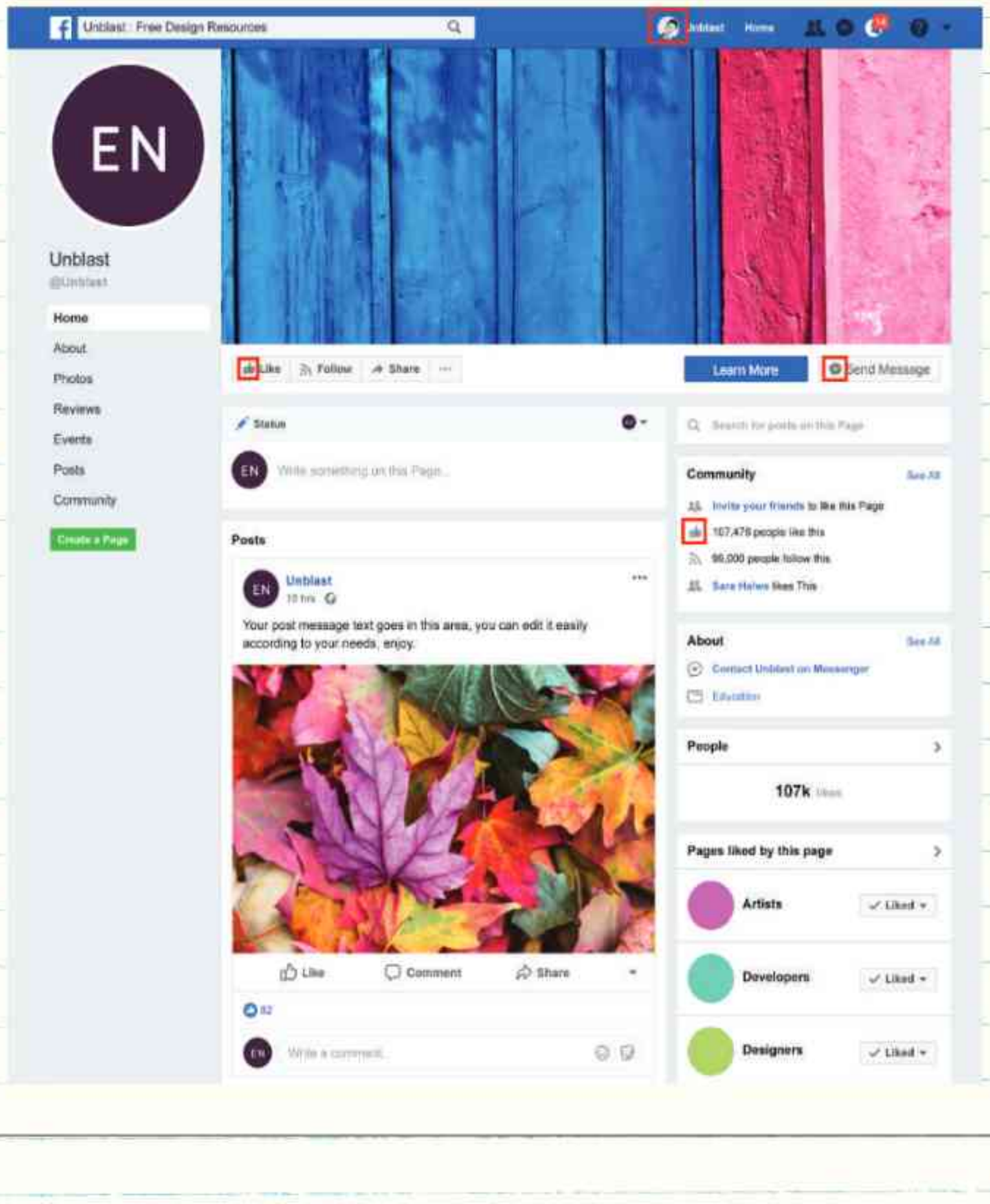
4. False.

E-Pathshala is a joint initiative of the Ministry of Human Resource Development (MHRD) and the National Council of Educational Research and Training d Windows platforms) .

5.True.

Digital literacy involves the ability to read, understand and interpret digital processes whereas, digital communication is the ability to communicate, connect and interact with others.

- ACTIVITY 2



DIGITAL COMMUNICATION

- **ACTIVITY 1**

These statements are not legitimate for the following reasons:

1. The sender seeks to bribe by offering bonus points.
2. The sender uses flattery to seek greater access to the recipient of the message.
3. The sender threatens to gain further access the recipient of message.
4. It reflects coercion of the recipient by a desensitised sender, which may increase in intensity.
5. The sender introduces subtle sexual allusions and sexualised game in the conversation to build intimacy, which may be manipulated further.

- **ACTIVITY 2**

1. One -way communication.
2. Flattery.
3. Gaming.
4. Revenge Pornography.

- **ACTIVITY 3**

The following preventive measures reduce the possibility of online risks and threats:

1. Always install a good antivirus software on your computer, smartphone and other handheld devices. Regularly update the antivirus and other applications.

2. Do not share personal information like name, date of birth, address or phone numbers while playing online games. Never share your passwords with anyone.

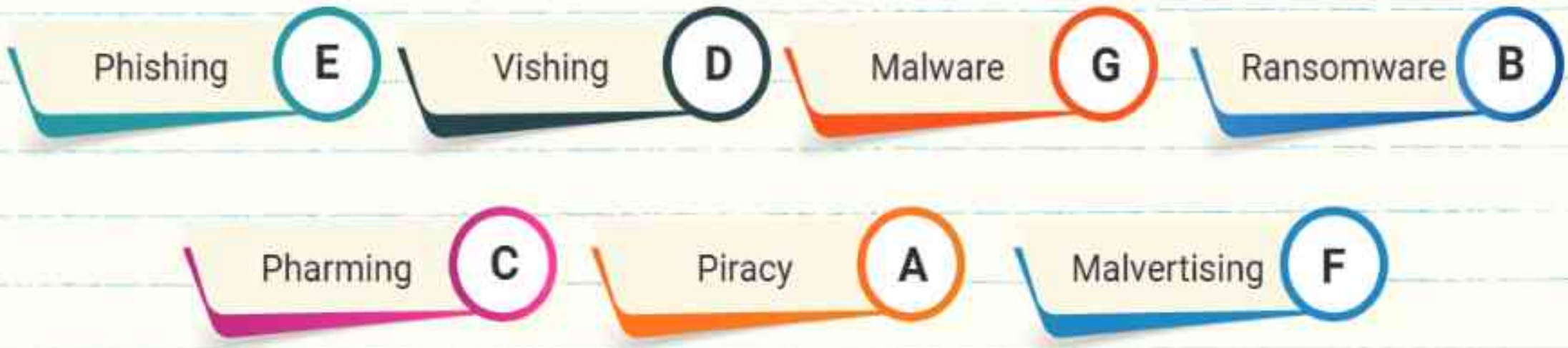
Use a complex password for online gaming and other online accounts. Change your password at regular intervals.

3. Never use voice chat or webcam while playing online games. This may reveal your identity to other players and attract cyber bullies and cyber criminals.

4. Never share your or your parent's credit card/debit card details with anyone while playing online games. You may be asked credit or debit card details but never share such details with anyone.

DIGITAL COMMERCE

- **ACTIVITY 1**



DIGITAL ETIQUETTE

- **ACTIVITY 1**

Cyberbullying takes place between two people. The cyberbullies, known people, known people hiding their identities, or strangers, send nasty text messages or emails, or set up hate groups on social networking sites. The victim is often targeted constantly, or periodically, even when they are in the comfort of their own home. The technologies enable the cyberbullies to circulate messages or images very quickly and widely on the internet.

Cyberstalking is when an individual is repeatedly or constantly followed, watched

or contacted through any electronic means, without his or her consent for sexual harassment or other mala fide motives. It involves tracking of the movement, invasion of privacy, or persistent efforts to establish contact through text, email, social media, or other digital platforms.

- **ACTIVITY 2**

1. Personal or private photos.
2. Location.
3. Mean or hurtful comments .
4. Date of birth.
5. Forwarded spam messages.
6. Mobile number.
7. Personal Details.

- **ACTIVITY 3**

1. Agree to disagree.
2. Avoid digital drama.
3. Be positive online.
4. Be responsible, honest and truthful.
5. Respect people's confidence.
6. Appreciate boundaries – your own and of others.
7. Learn to seek consent.

- **ACTIVITY 4**

1. Making fun of another user in internet chat rooms.
2. Harassing a user over instant messaging sessions.
3. Posting derogatory messages on a user's social networking pages.
4. Circulating rumours about someone on social networks.
5. Publishing lewd comments about another person on personal blogs.
6. Posting unflattering pictures of another user on the web.
7. Sending unsolicited and unwanted email messages (also known as spamming).

8. Sending threatening or provocative emails.
9. Repeatedly phoning another person.

- **ACTIVITY 5**

1. Search yourself online to see how you appear to others.
2. Check privacy settings to ensure that only people authorised by you are able to access your posts.
3. Deactivate and delete - WHAT.

DIGITAL RIGHTS

- **ACTIVITY 1**

E A family friend is blackmailing you into sending inappropriate images to him.

D Your friend posts a picture of you without consulting you. When asked to remove the picture they refuse.

A On social media you have someone who stalks you and you want to make a complaint.

B A sport organisation does not let you apply for its online cricket training programme because you belong to a lower socio-economic background.

C Your school library bans an educational book that is appropriate for your age group.

DIGITAL SECURITY

- **ACTIVITY 1**

Internet safety crossword:

1. VIRUS
2. ANTIVIRUS
3. FIREWALL
4. CYBERBULLYING
5. PHISHING

- **ACTIVITY 2**

Word search

1. Phishing
2. Virus
3. Malware
4. Cloud
5. WAF
6. Firewall

- **ACTIVITY 3**

1. (a) An$#yOuM@n!071
2. (d) All of the above

- **ACTIVITY 4**

1. Keep webcams private.
2. USB Storage Device Use.
3. Regularly update software and operating systems.

- ACTIVITY 5

Stalkerware refers to software applications that are designed to track or spy on individuals without their knowledge and consent.

DIGITAL LAW

- ACTIVITY 1

1. Plagiarism: Imprisonment for a term ranging between 6 months and 3 years, and fine.
2. Impersonation: Imprisonment up to 3 years and a fine.
3. Revenge porn: Imprisonment up to 7 years with a fine. In case the act has serious consequences, e.g., suicide or attempted suicide, it may even attract a life term.
4. Unauthorised access: Imprisonment up to 2-3 years, or fine, or both.
5. Defamation: Imprisonment up to 2-3 years, or fine, or both.

- ACTIVITY 2

1. Choose your friends wisely.
2. Think before you say or post anything.
3. Be aware of the dangers of sharing.
4. Be alert to suspicious activities.
5. Manage how you appear to others. Being positive online also secures your digital footprints.
6. Block or report unwanted contacts.
7 “Untag” yourself from posts and pictures that you do not .
8. Be cautious while accepting followers.
9. tManage your privacy settings.

- **ACTIVITY 3**

The complaint may be lodged on the social media platform, the Ministry of Home Affairs portal, with the local police and police cybercell, and e-Raksha portal at the NCPCR website.

USEFUL CONTACTS

Lodge complaints in person, by post, by messenger, or by any means to the following address:

National Commission for the Protection of Child Rights (NCPCR),
5th Floor, Chandralok Building, 36 Janpath,
New Delhi 110 001

Complaints can be lodged through E-Raksha, or delivered in by post or in person at the above address.

Nodal CyberCrime Portal			
Name	**Rank**	**Landline**	**Email**
Ms. D Mary Prasanthi	SP	0863-2340063	cybercrimes-cid@ap.gov.in
Sh. Jimmy Chiram	SP	0360-2212471	spcr@arunpol.nic.in, spsit@arunpol.nic.in
Sh. Debajit Hazarike	DIGP	0361-2529840	digp-cid@assampolice.gov.in
Sh. D.Amarcase	ASP	0612-2216236	cybercell-bih@nic.in
Manisha Thakur R	AIGP	0771-2511606	aigtech-phq.cg@gov.in
Sh. Karthik Kashyap	SP	0832-2443082	picyber@goapolice.gov.in spcyber@goapolice.gov.in
Sh. Rajesh GadhiyaSI	SPDSI	079-23255545	cc-cid@gujarat.gov.in
Sh. Ashwin Shenvi	SP	01733-253023	sp.crime2pkl@hry.nic.in
Sh. Narveer Rathore	DSP	0177-2621331	polcyberps-shi-hp@nic.in
Sh. Syed Ahfadul-ul-I	IGP	0191-2572475	igcrime@jkpolice.gov.in igcrime-jk@nic.in
Sh. Sunil BhaskarSh.	SPDSI	0651-22100580651-22	cyberps@jhpolice.gov.in
Sh. Chandra GuptaSh.	SPDSI	080-22094436	spccpscid@ksp.gov.in ccps@kar.nic.in
Sh. Sreejith	IGP	0471-2319787	igpcrimes.pol@kerala.gov.in cyberps.pol@kerala.gov.in
Sh. Niranjan B Vayanrg	DIGPA	755-2443483	mpcyberpolice@mppolice.gov.in aig1cybercell@mppolice.gov.in niranjan.vayangankar889@mppolice.gov.in
Sh. Balsing Rajput	SP	022-22160080	sp.cbr-mah@gov.in control.cpaw-mah@gov.in apl1.cpaw-mah@gov.in
Ms. Joyce Lalremmaw	SP	0385-2451501	cidcb-mn@nic.in cybercrime.mn@gov.in
Sh. R. Muthu	SP	0364-2504416	r.muthu@ips.gov.in ccw-meg@gov.in
Sh. Zosangliana	SP	0389-2334082	cidcrime-mz@nic.in
Ms. Sonia Singh	IGP	0370-2242712	cybercrimeps-ngl@gov.in
Sh Anil Kumar Dash	ASP	0671-2974401	sp1cidcb.orpol@nic.in dirscrb.odpol@nic.in
Sh. Dhruman Harshar	AIG	0172-2226258	aigcc@punjabpolice.gov.in
Sh. Pankaj Chaudhary	SP	0141-2740169	ccps-raj@nic.in
Sh. Prathap Pradhan	DIGP	03592-202087035 92	spcid@sikkimpolice.nic.in
Ms. B.Shamoondeswa	SP	044-28512527	spcybercbcid.tnpol@nic.in cbcyber@nic.in
Sh. Govind SinghSh. I	ADGP	040-23242424	adg_cid@tspolice.gov.in ccps.cid@tspolice.gov.in
Ms.Sarswati R IPS	IPS	0381-2304344	spcybercrime@tripurapolice.nic.in
Sh. Barinderjit Singh	SSP	0135-2651689	spstf-uk@nic.in ccps.deh@uttarakhandpolice.uk.gov.in
Sh. Vivek Ranjan	DSP	0522-2721690	ccpsnoida@upstf.com
Sh. Rajesh Kumar Yao	DIGP	033-24792955	ccpwb@cidwestbengal.gov.in digcyber@cidwestbengal.gov.in
Sh. Sanjay Kumar	IGP (A)	03192-232334	igpint.and@nic.in
Ms. Rashmi Sharma Y	DSP	0172-2710046	dspccic.chd@nic.in police-chd@nic.in
Sh. Anyesh Roy	DCP	011-23746615	acp-cybercell-dl@nic.in acp.cybercell@delhipolice.gov.in
Sh. Vipul Anekant	ASP	0260-2254101	sdpo-diu-dd@nic.in sebastian.devasia@gov.in
Sh. Manasvi Jain	Dy. SP	0260-2632888	dysp-hq-dnh@gov.in / For correspondence - itcell-dnhp@mha.gov.in
Sh. Mahesh kumar Ba	SSP	0413-2224083	cybercell-police.py@gov.in sspci.pon@nic.in
Sh. Mayank Bansal	DSP	04896-262367	

Grievance Officer Details			
Name	**Rank**	**Landline**	**Email**
Sh. J Prabhakar Ra	DIGP	0863-2340152	cybercrimes-cid@ap.gov.in
Sh. Take Ringu	DIGP	0360-2215518	sit@arunpol.nic.in
Sh. Surendra kuma	IGP	0361-2524494	igp-cid@assampolice.gov.in
Sh. Shiv Kumar Jha	DIG	0612-2238098	dig-bih@nic.in
Sh. R K Vij	SPL DGP	0771-2511623	vijrk@gov.in
Sh. Paramaditya	DIGP	0832-2420883	digpgoa@goapolice.gov.in
Sh. Ajay Tomar	ADGP	079-23250798	cc-cid@gujarat.gov.in
Sh. Kuldip Singh Si	ADGP	01733-253230	igp.crime2-hry@nic.in
Sh. Sandeep Dhaw	SP	0177-2627955	sp-cybercr-hp@nic.in
Sh. B Srinivas	ADGP	0191-2582996	adgpcidjk@jkpolice.gov.in
Sh. Ranjit Prasad	IGP	0651-2490046	ig-orgcid@jhpolice.gov.in
Sh. T D Pawar	DIGP	080-22251817	digadmincod@ksp.gov.in
Sh. Dr. Shaik Darve	ADGP	0471-2722215	adgpcrimes.pol@kerala.gov.in
Smt. Aruna Mohan	SPL DGP	0755-2770248	spl.dgp-cybercell@mppolice.gov.in
Sh. Brijesh Singh	SPL IGPA	022-22026672	ig.cbr-mah@gov.in
Sh. Themthing Nga	DIGP	0385-2450573	themthing.ng@gov.in
Sh. F G Kharshiing	DIGP	0364-2550141	fg.kharshiing@ips.gov.in
Sh. Balaji Srivastav	DGP	0389-2334682	polmizo@rediffmail.com
Sh. Renchamo P. K	ADGP	0370-2223897	renchamo.p@gov.in
Sh. Madkar Sandee	SP	0671-2306071	sp1cidcb.orpol@nic.in
Sh. Hardial Singh M	DIGP	0172-2226258	aigcc@punjabpolice.gov.in shocc@punjabpolice.gov.in
Sh. Sharat Kaviraj	DIGP	0141-2740898	sharat.kaviraj@rajasthan.gov.in
Sh. Sonam Detchu	DySP	03592-204297	spcid@sikkimpolice.nic.in
Sh. C Sridhar	IGP	022-28512503	cbcyber@nic.in
Smt. Swathi Lakra	IGP	040-23147604	igp_wpc@cid.tspolice.gov.in
Sh. Subrata Chakra	AIGP	0381-2304344	aigcrime@tripurapolice.nic.in
Sh. Deepam Seth	IGP	0135-2712563	dgc-police-ua@nic.in
Dr. Kalluri SP Kuma	ADGP	0522-2208598	ccpsnoida@upstf.com
Sh. Ashok Kumar P	IGP	033-24791830	ig2@cidwestbengal.gov.in
Smti. Shalini Singh	IGP (L&O)	03192-232244	igplo.and@nic.in
Ms. Nilambari Jagao	SSP	0172-2760001	pssput-chd@nic.in
Sh. Prem Nath	ACP	011-23490236	jtcp-ops-dl@delhipolice.gov.in
Sh. Vikramjit Singh	SP	0260-2250942	sp-dmn-dd@nic.in
Sh. Sharad B. Dara	SP	0260-2643022	sp-sil-dnh@nic.in
Sh. Dr. VJ Chandra	DIGP	0413-2231386	dig.pon@nic.in
Sh. Shibesh Singh	SSP	04896-262258	lak-sop@nic.in

USEFUL RESOURCES

* https://www.cyberpeacecorps.in/CPCRC/

* Government of India, Ministry of Home Affairs. A Handbook for Adolescents/Students on Cyber Security. https://mha.gov.in/sites/default/files/CyberSafety_English_Web_03122018_0.pdf

* Being Safe Online: Guidelines for raising Awareness among children, parents, educators and the general public **https://ncpcr.gov.in/showfile.php?lang=1&level=1&&sublinkid=1637&lid=1661**

CBSEIndia | cbseindia29 | cbse_hq_1929

Cyberpeacecorps

Cyber Peace Foundation