VISVESVARAYA TECHNOLOGICAL UNIVERSITY

"Jnana Sangama", Belagavi, Karnataka, India.

A Report

On

AICTE ACTIVITY POINT PROGRAMME

Submitted in partial fulfillment of the requirement for the award of the degree of

Bachelor of Engineering

in

Information Science and Engineering

Submitted By

K SAI SHARAN REDDY

1DT19IS053

AICTE Department Coordinator

Prof. Spandana S G

Assistant Professor,

Dept. of ISE

Department of Information Science and Engineering

(Accredited by NBA 2022-2025)

DAYANANDA SAGAR ACADEMY OF TECHNOLOGY AND MANAGEMENT

Kanakapura Road, Udayapura, Bengaluru- 560082

2022–2023

DAYANANDA SAGAR ACADEMY OF TECHNOLOGY AND MANAGEMENT

Department of Information Science and Engineering

Bengaluru – 560082

CERTIFICATE

This is to certify that **K SAI SHARAN REDDY**, bearing **1DT19IS053** of 8th semester has completed "AICTE ACTIVITY PROGRAM" in partial fulfillment for the award of degree in Bachelor of Engineering in **Information Science and Engineering** of the Visvesvaraya Technological University, Belagavi during the year 2019-2023. It is certified that all corrections/suggestions indicated for internal assessment have been incorporated in the report deposited in the department library. The project report has been approved as it satisfies the academic requirements for Bachelor of Engineering Degree.

Dr. Pooja Nayak S
Assistant Professor
Dept. of ISE
DSATM, Bengaluru

Dr. Nandini Prasad K S
Dean - Foreign Affairs & Head
Dept. of ISE
DSATM, Bengaluru

ACKNOWLEDGEMENT

The satisfaction and the euphoria that accompany the successful completion of any task would be incomplete without the mention of the people who made it possible. The constant guidance of these persons and encouragement provided, crowned our efforts with success and glory. Althoughit is not possible to thank all the members who helped for the completion of the AICTE Activity work individually, I take this opportunity to express my gratitude to one and all.

I am grateful to the management and our institute **DAYANANDA SAGAR ACADEMY OF TECHNOLOGY AND MANAGEMENT** with its very ideals and inspiration for having provided me with the facilities which made this work a success.

I express my sincere gratitude to **Dr. M Ravishankar**, Principal, Dayananda Sagar Academy of Technology and Management for the support and encouragement.

I wish to place on record, my grateful thanks to **Dr. Nandini Prasad K S**, Dean-Foreign Affairs and HoD-ISE, Dayananda Sagar Academy of Technology and Management, for the constant encouragement provided to me.

I am indebted with a deep sense of gratitude for the constant inspiration, encouragement, timely guidance and valid suggestion given to me by my guide **Dr. Pooja Nayak S, Assistant Professor**, Departmentof ISE, Dayananda Sagar Academy of Technology and Management.

I am thankful to all the staff members of the department for providing relevant information and helped in different capacities in carrying out this AICTE activity work.

Last, but not least, I owe my debts to my parents, friends and also those who directly or indirectly have helped me to make the AICTE a success.

K Sai Sharan Reddy [1DT19IS053]

ACADEMIC YEAR AND BATCH (2019-2023)

NAME OF THE STUDENT			**K SAI SHARAN REDDY**			
STUDENT USN			**1DT19IS053**			
SEMESTER AND SECTION			**8TH A**			
REGULAR/ REPEATER/ LATERAL ENTRY			**REGULAR**			
TITLE OF ACTIVITY	**PLACE OF ACTIVITY**	**DATES OF ACTIVITY**	**HOURS OF ACTIVITY**	**MAXIMUM POINTS**	**POINTS SECURED**	**REMARKS**
SPREADING PUBLIC AWARENESS UNDER RURAL OUTREACH PROGRAMME	**Thittahalli**	**23-06-22 to 29-06-22**	**80**	**20**		
CONTRIBUTION TO ANY NATIONAL LEVEL INITIATIVE OF GOVERNMENT OF INDIA	**Mukkodlu**	**19-02-23 to 01-03-23**	**80**	**20**		
TOURISM PROMOTION INNOVATIVE APPROACHES	**Dodda hoskote Lake**	**20-03-23 to 26-03-23**	**80**	**20**		
SETTING OF THE INFORMATION IMPARTING CLUB FOR WOMEN LEADING TO CONTRIBUTION IN SOCIAL AND ECONOMIC ISSUES	**Dayananda Sagar Academy of Technology and Management**	**27-11-22 to 10-12-22**	**80**	**20**		
TOTAL ACTIVITY POINTS SECURED						

SIGNATURE OF THE STUDENT	**NAME AND SIGNATURE OF THE PROCTOR**	**NAME AND SIGNATURE OF HEAD OFTHE DEPARTMENT**

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

SPREADING PUBLIC AWARENESS UNDER RURAL OUTREACH PROGRAMME

TASK PERFORMED

DURATION:80 hrs(23rd June 2022 to 29th June 2022)

Activity start date: 23 June 2022

DAY 1: 23rd June 2022

We have prepared templates/Posters on this day.Posters give pictorial representation which is helpful for easy explanation.

DAY 2: 24th June 2022

This day we were taken to a village named thittahalli and Mukkodlu which belonged to Somanahalli panchayat where we prepared banners related to less usage of plastic and they reached out homes and public and each of the team explained them the effect of using more plastic.

DAY 3: 25th June 2022

We have explained the importance of plastic free environment on this day.

DAY 4: 26th June 2022

We have performed many activities to show how plastic harms our environment.

DAY 5: 27th June 2022

They also explained them the future problems that will occur due to usage of more plastic.This program has brought us a lot of information about creating awareness and talking to people. We reached homes of the people living in those areas and explained our views on usage of plastic and also created very good awareness in the society.

DAY 6: 28th June 2022

We have told them about 4 R's:Reduce, Reuse, Recycle and Recover & its importance.

DAY 7: 29th June 2022

On final day of session finally we have completed our moto of making the village aware about plastic free environment.

About the activity:

An outreach program aims to help, uplift, and support those who are deprived of certain services and rights. It involves giving learning, social planning, health support, and other projects for their welfare. As usual, a program must be organized to use resources and aid to fulfill a goal. Successful community outreach programs must have project leaders at their core. They take charge of promoting, searching for donors and volunteers, and recording details about the outreach. Planning programs for the community can help solve a greater need for a long-term plan toward social progress. Further, other program members must join hands to plan and source out more assets and means to create more long-term solutions and voluntary efforts. Having that said; why the need to start or join an outreach program? The main purpose is to help achieve a goal for the greater good. This is by choosing a specific group, analyzing their needs on certain issues, and therefore building a program to aid them in learning, recovering, or becoming self-sufficient. Rural Outreach Development Rural development usually refers to the method of enhancing the quality of life and financial well-being of individuals, specifically living in populated and remote areas. Traditionally, rural development was centred on the misuse of land-intensive natural resources such as forestry and agriculture. However today, the increasing urbanisation and the change in global production networks have transformed the nature of rural areas. Rural development still remains the core of the overall development of the country. More than two-third of the country's people are dependent on

As a part of an AICTE Activity we were taken out to a rural area to create public awareness about reducing the use of plastic. It was such a great initiative taken by the department to promote awareness on the most important topic. These days we were taken to a village named thittahalli and Mukkodlu which belonged to Somanahalli panchayat where we prepared banners related to less usage of plastic and they reached out homes and public and each of the team explained them the effect of using more plastic. also explained them the future problems that will occur due to usage of more plastic.This program has brought us a lot of

information about creating awareness and talking to people. We reached homes of the people living in those areas and explained our views on usage of plastic and also created very good awareness in the society.The department has given us such an amazing opportunity to portray ourselves as something unique apart from academics.We have learned values and how to promote awareness.

BENEFITS OF RURAL OUT REACH PROGRAM

- Educate: These aim to give educational support for children and out-of-school individuals. This relates to the goal to help uproot poverty on a larger scale.

- Inspire and uplift: Through various types of outreach programs, these also build avenues where people can thrive with support and with others. Being stewards of inspiration and Bayanihan encouragement contribute to building empowered stewards of change!

- Bring joy: For volunteers, an outreach program relieves them from a lot of stress. Donors and volunteers feel more at peace and fulfilled knowing they've done their part; while recipients feel they're not alone in their journey. No matter the main purpose of your effort to give back to those in need, we only arrive at one key goal: to build more ways and paths for the betterment of our society.

Snapshots/Pics:

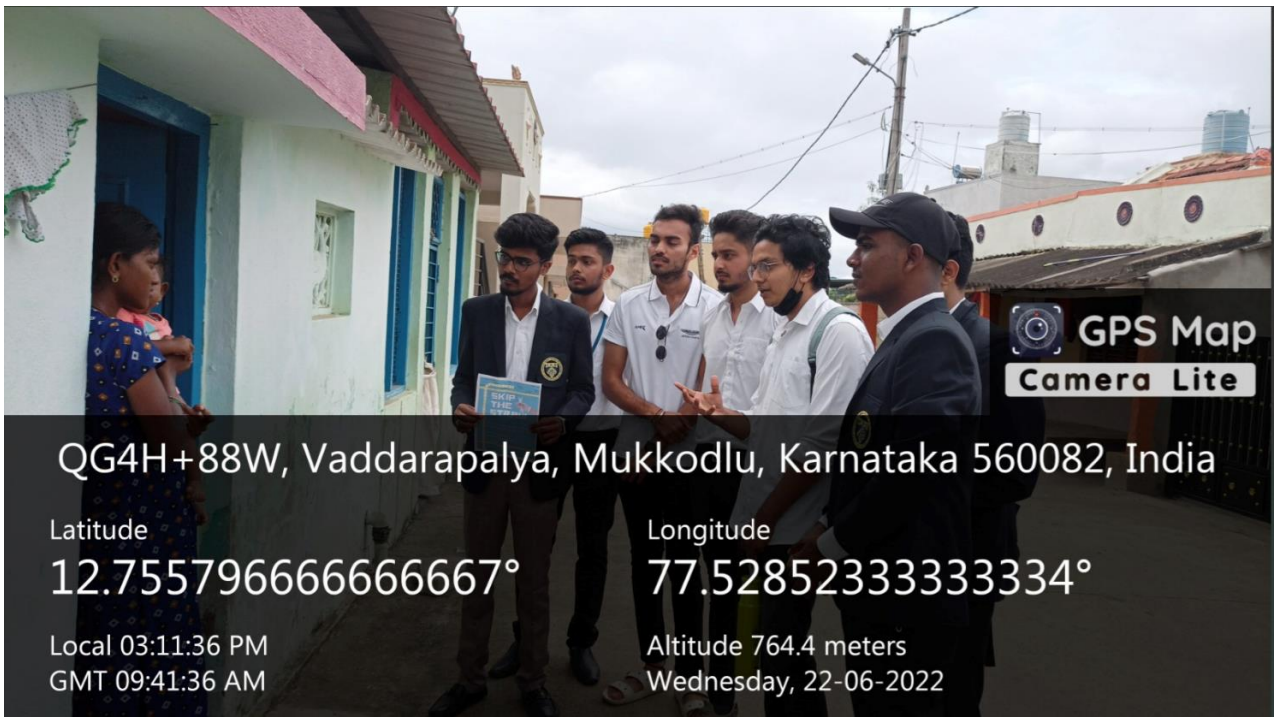


Fig 1.1 meeting a localite

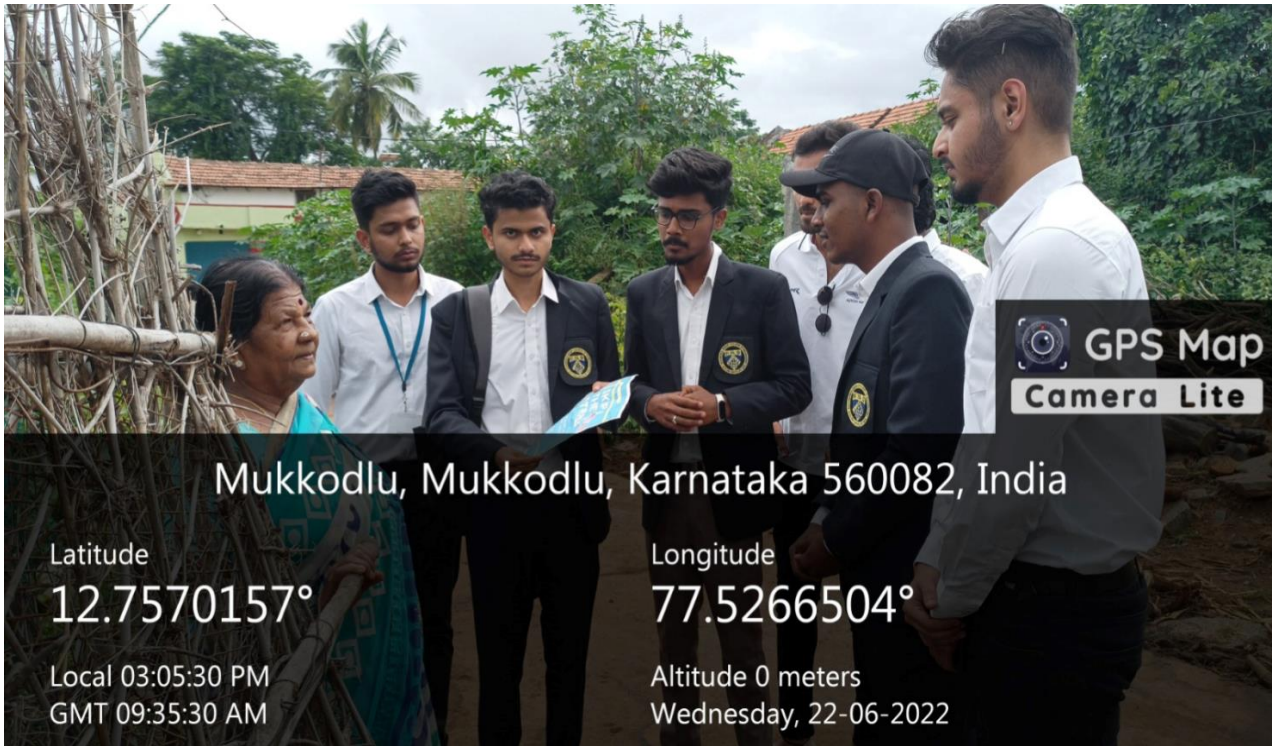


Fig 1.2 showing the interaction with the nearby people

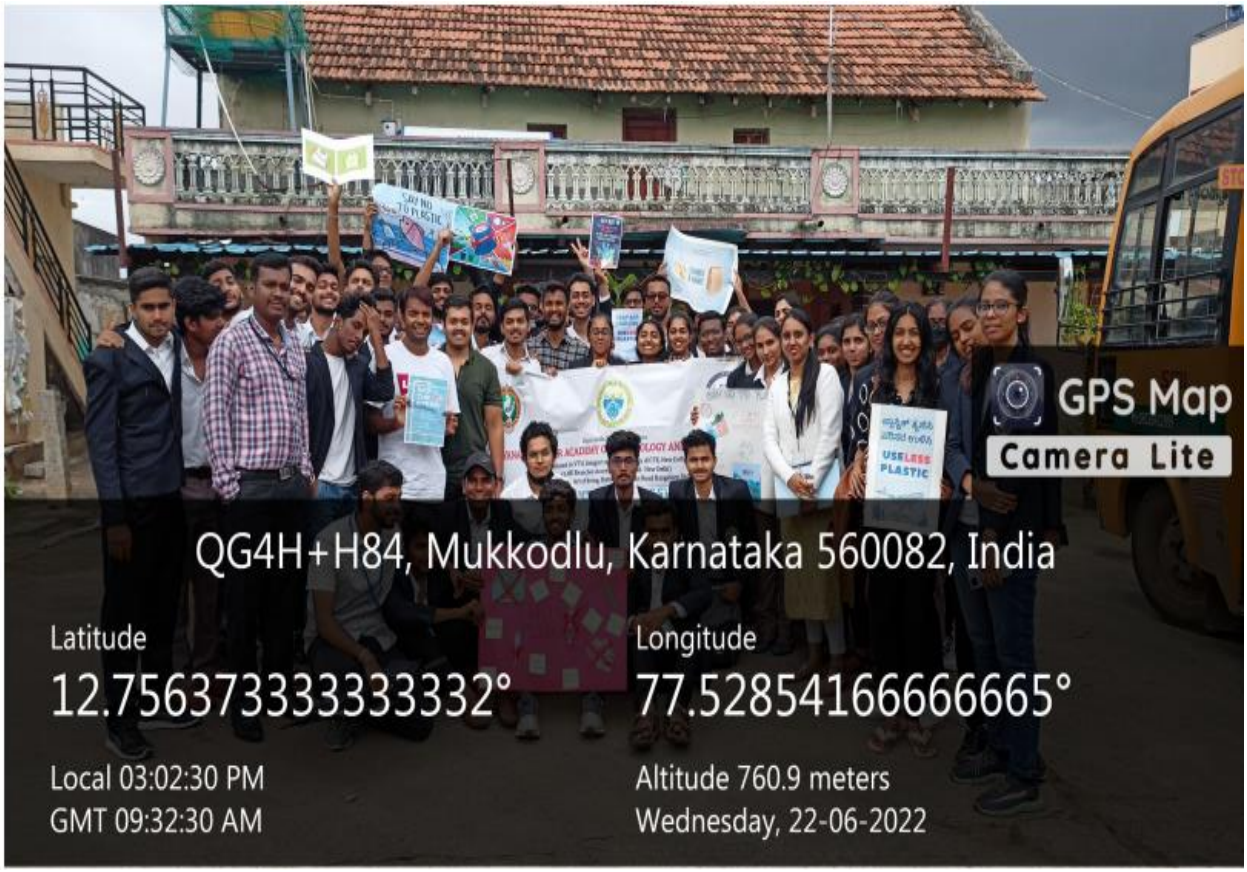


Fig 1.3 showing the teamwork required for awareness program

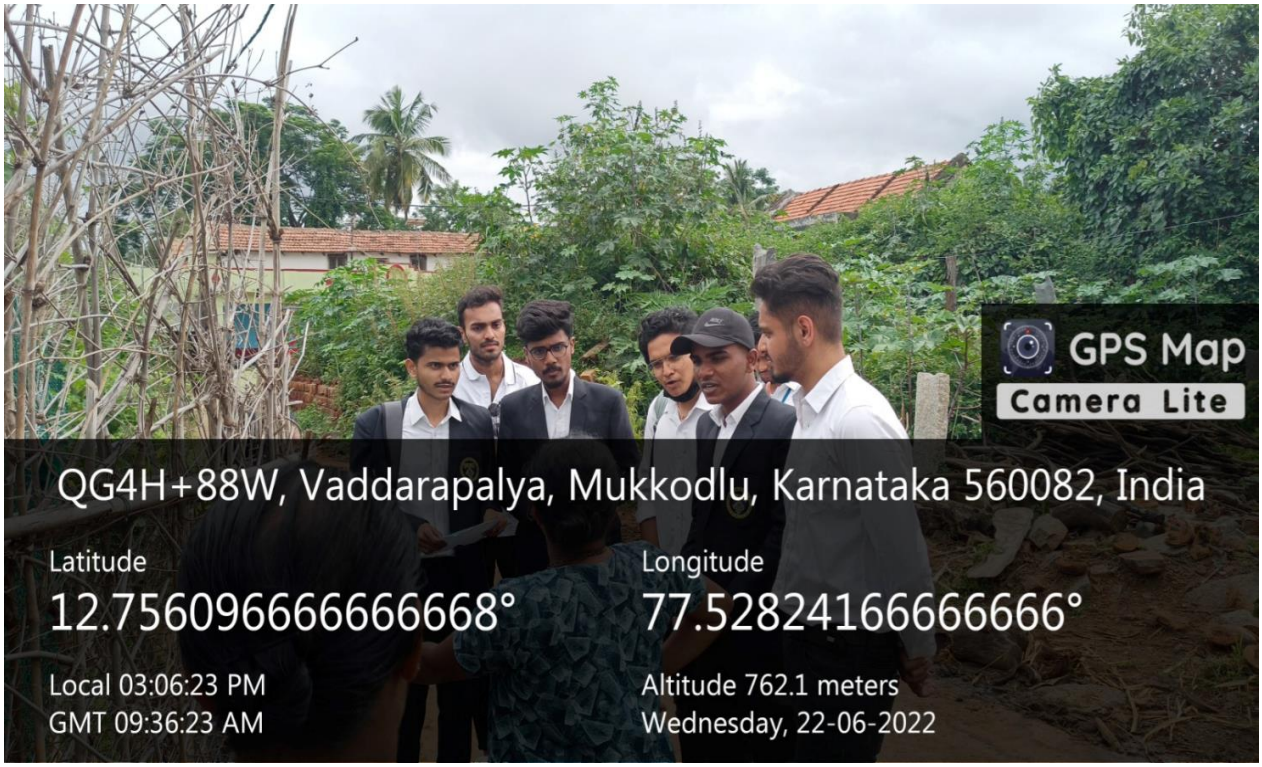


Fig 1.4 showing the talk with the local area vendor

CHAPTER 2

CONTRIBUTION TO ANY NATIONAL LEVEL INITIATIVE OF GOVERNMENT OF INDIA

Duration:80 hrs(19th Feb to 1st March 2023)

Contributing to the **Swachh Bharat** national level initiative of the Government of India involved several planning and scheduling activities. Here is the outline:

2.1 PLANNING AND SCHEDULING OF THE ACTIVITY

1. Identifying the scope of the initiative: Define the scope of the initiative in terms of the specific goals and objectives, such as promoting cleanliness and hygiene, reducing waste, and improving sanitation.
2. Conducting a needs assessment: Conduct a needs assessment to identify the specific areas and communities that require attention and support. This can be done by conducting surveys, consulting with local stakeholders, and reviewing available data and reports.
3. Developing a plan of action: Based on the needs assessment, develop a comprehensive plan of action that outlines the specific activities and resources required to achieve the identified goals and objectives.
4. Securing funding and resources: Identify and secure the necessary funding and resources to support the implementation of the plan of action, including staff, equipment, and materials.
5. Mobilizing stakeholders: Engage with local communities, government agencies, and other stakeholders to raise awareness and support for the initiative. This can be done through various communication channels, such as social media, public meetings, and outreach programs.
6. Implementing the plan: Execute the plan of action by carrying out the identified activities, such as cleaning up public spaces, improving sanitation facilities, and promoting waste reduction and recycling.
7. Monitoring and evaluation: Regularly monitor and evaluate the progress and impact of the initiative to identify any areas for improvement and adjust the plan of action as needed.

Overall, contributing to the Swachh Bharat national level initiative requires a systematic and coordinated approach that involves careful planning and scheduling of activities, as well as effective stakeholder engagement and ongoing monitoring and evaluation.

2.2 DESCRIPTION OF THE ACTIVITY CONDUCTED

Contributing to the Swachh Bharat national level initiative of the Government of India involved various activities, depending on the specific goals and objectives of the initiative. Here are some of the activities that was conducted:

1. Cleaning up public spaces: One of the primary goals of the Swachh Bharat initiative is to promote cleanliness in public spaces. Activities such as organizing community clean-up drives, installing waste bins, and promoting responsible waste disposal can help to achieve this goal.
2. Improving sanitation facilities: Another key aspect of the Swachh Bharat initiative is to improve sanitation facilities in communities. Activities such as building public toilets, promoting the use of toilets, and providing clean water sources can help to achieve this objective.
3. Promoting waste reduction and recycling: The Swachh Bharat initiative also aims to reduce waste and promote recycling. Activities such as organizing awareness campaigns, conducting waste audits, and promoting the use of composting can help to achieve this objective.
4. Engaging with local communities: Engaging with local communities is critical to the success of the Swachh Bharat initiative. Activities such as conducting outreach programs, involving local leaders and volunteers, and organizing public meetings can help to raise awareness and support for the initiative.
5. Implementing government policies and regulations: The success of the Swachh Bharat initiative also depends on effective implementation of government policies and regulations related to waste management and sanitation. Activities such as conducting regular inspections, enforcing rules and regulations, and providing training to government staff can help to achieve this objective. Overall, contributing to the Swachh Bharat national level initiative of the Government of India requires a multi-faceted approach that involves various activities aimed at promoting cleanliness, improving sanitation, and reducing waste.

2.3 OUTCOME OF THE ACTIVITY

The outcome of contributing to the Swachh Bharat national level initiative of the Government of

India can be significant in promoting cleanliness, improving sanitation, and reducing waste in communities. Here are some possible outcomes of the activities mentioned earlier:

1. Improved public spaces: Organizing community clean-up drives, installing waste bins, and promoting responsible waste disposal can help to improve the cleanliness of public spaces such as parks, streets, and public buildings.
2. Better sanitation facilities: Building public toilets, promoting the use of toilets, and providing clean water sources can help to improve sanitation facilities in communities. This can lead to a reduction in water-borne diseases and improve overall health and hygiene.
3. Reduced waste and increased recycling: Promoting waste reduction and recycling can help to reduce the amount of waste generated and promote sustainable waste management practices. This can also help to reduce environmental pollution and conserve natural resources.
4. Increased community engagement: Engaging with local communities can help to raise awareness and support for the Swachh Bharat initiative. This can lead to increased community participation in waste management and sanitation activities, and help to build a sense of ownership and responsibility for keeping public spaces clean.
5. Effective implementation of policies and regulations: Implementing government policies and regulations related to waste management and sanitation can help to ensure that the Swachh Bharat initiative is successful in achieving its goals. This can help to improve overall waste management practices and promote sustainable development. Overall, the outcome of contributing to the Swachh Bharat national level initiative of the Government of India can have a positive impact on communities by improving cleanliness, sanitation, and waste management practices.Today, as the world searches for solutions to global climate change, tree planting has become more popular than ever. It’s a simple and appealing response to an overwhelming, existential crisis, and it makes for easy messaging: anyone can go out and plant a tree to help restore balance to Earth’s climate. But for many large-scale tree-planting

initiatives, the focus is on the number of new trees that end up in the ground, not on planting the right trees in the right places or caring for them after planting to ensure they survive. While mitigating climate change is the chief driver of many tree-planting initiatives, these projects often have other environmental goals, too, like regulating water cycles, halting soil erosion and desertification, and restoring wildlife habitat. They also often have socioeconomic goals, like alleviating poverty and enhancing local communities' health and livelihoods.

SNAPSHOTS

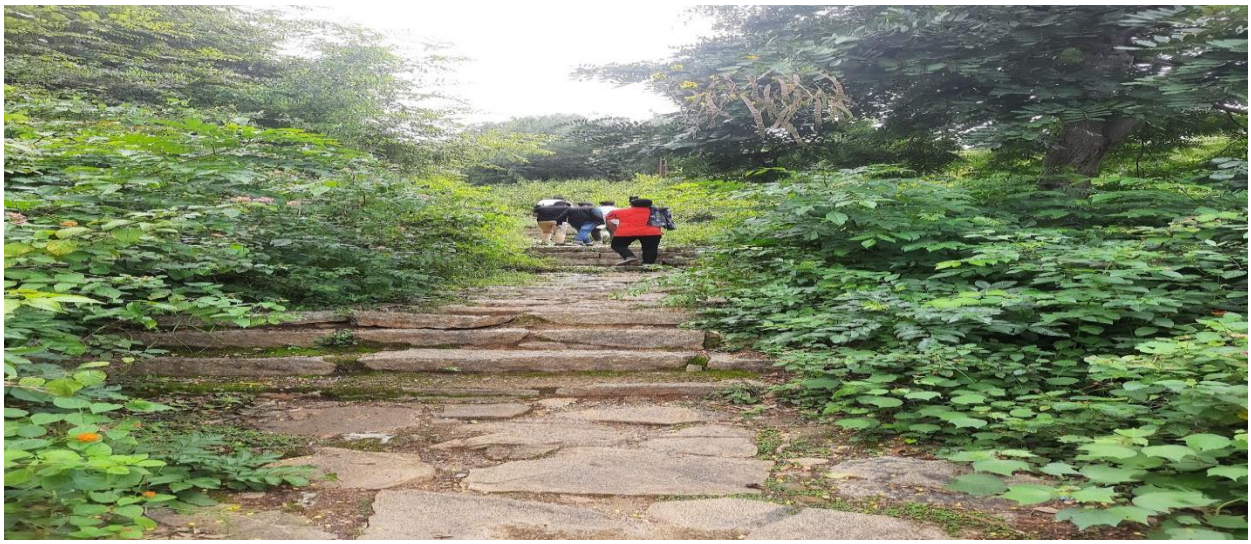


Fig 2.1 Cleaning the areas

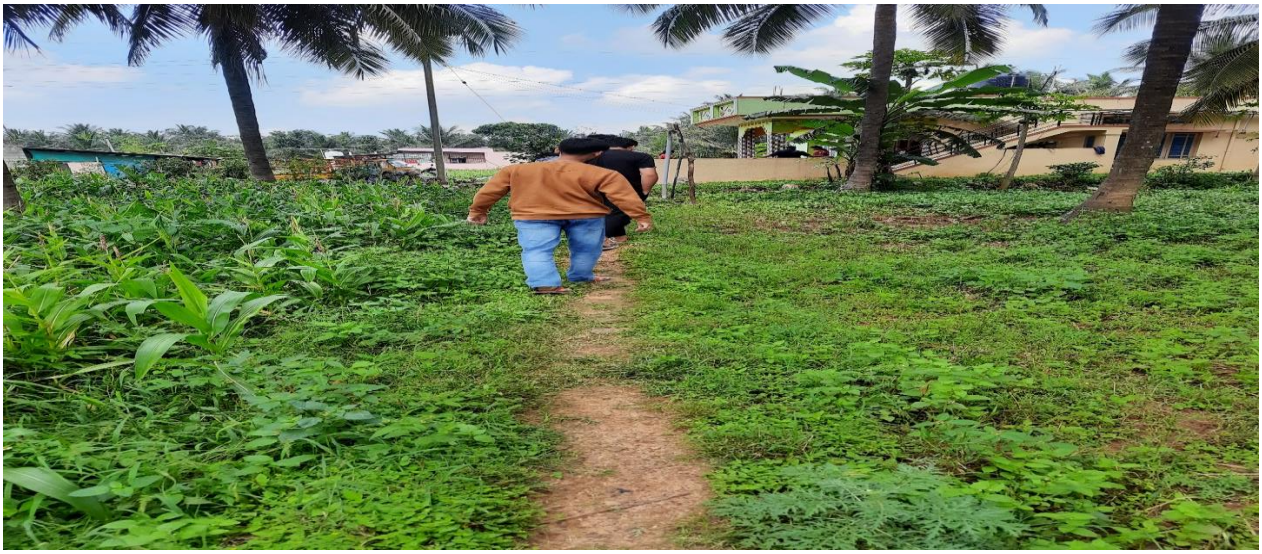


Fig 2.2 Conducting survey

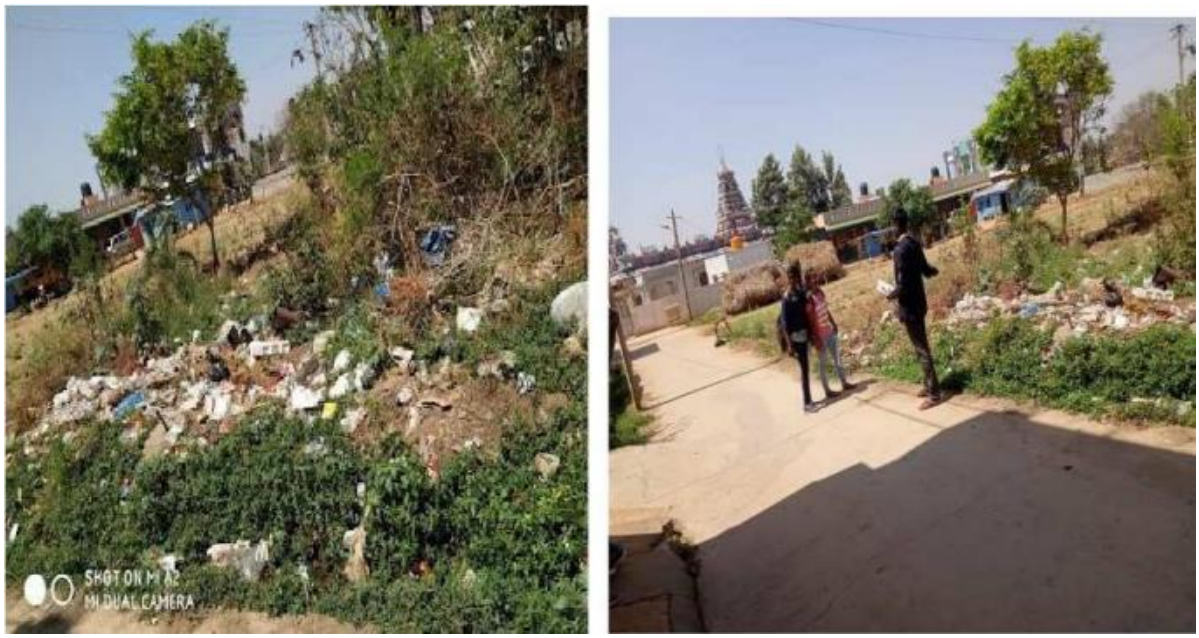


Fig 2.3 Removing Plastics

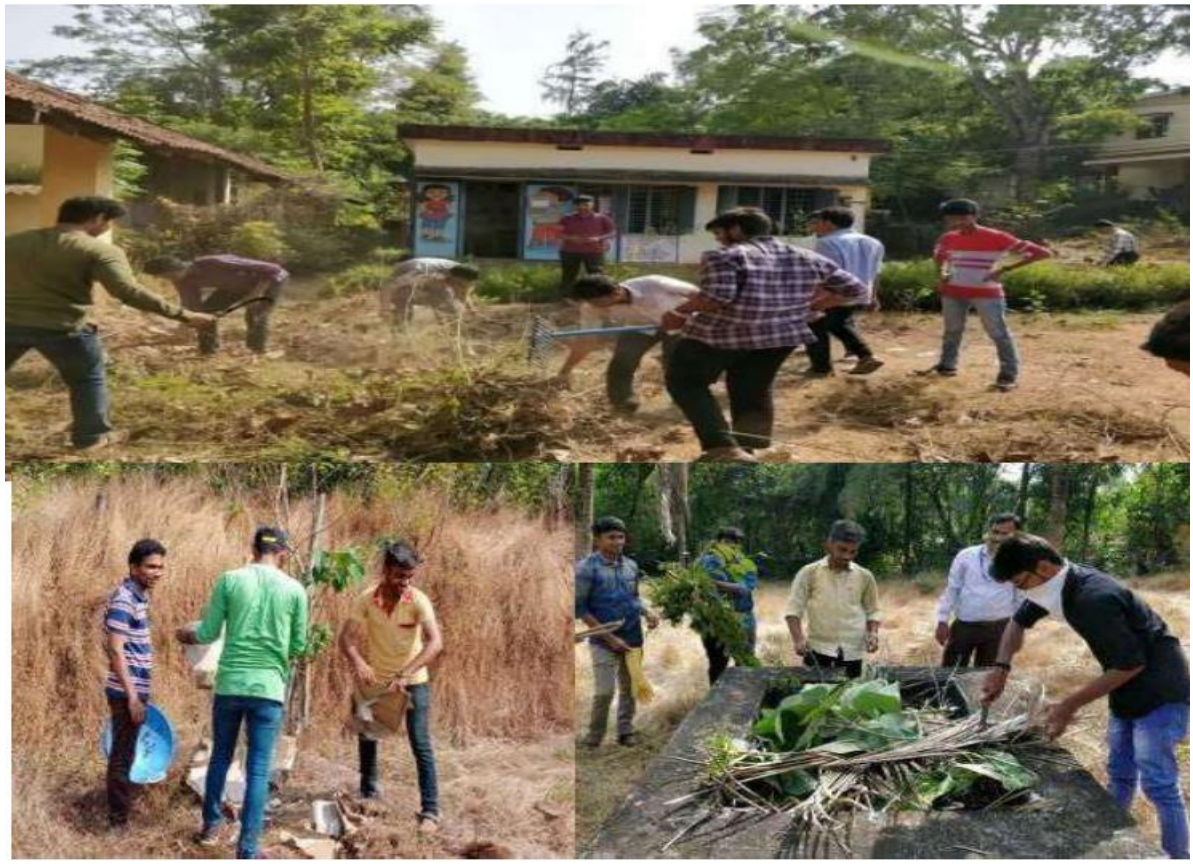


Fig 2.4 Garbage disposal

CHAPTER 3

Tourism Promotion Innovative Approaches and conducted a survey on Tourism places

Duration:80 hrs(20th Mar to 26th Mar 2023)

3.1ABOUT THE ACTIVITY

I have created awareness on Tourism Promotion Innovative Approaches and conducted a survey on Tourism places and automated local activities in Hoskote Taluk near Dodda Hoskote Lake, Hoskote Taluk, Bangalore Rural.

3.2 Description of Activity

Dodda Hoskote Lake is located in Hoskote Taluk in the state of Karnataka, India. There are several tourist places near the lake that visitors can explore. Here are some of the popular tourist attractions near Dodda Hoskote Lake:

1.Sri Chokkanathaswamy Temple: This ancient temple is located in Hoskote town, about 4 km from the lake. The temple is dedicated to Lord Vishnu and is known for its beautiful architecture and intricate carvings.

2.Nandi Hills: Nandi Hills is a popular hill station located about 55 km from Dodda Hoskote Lake. The hill station is known for its scenic beauty, pleasant weather, and historical significance. Visitors can enjoy activities like trekking, camping, and sightseeing at Nandi Hills.

3.Devanahalli Fort: Devanahalli Fort is a historic fort located about 32 km from the lake. The fort was built in the 16th century and is known for its architectural beauty and historical significance. Visitors can explore the fort and learn about its rich history.

4.Muddenahalli: Muddenahalli is a small town located about 19 km from Dodda Hoskote Lake. The town is famous as the birthplace of Sir M. Visvesvaraya, a renowned engineer and

statesman. Visitors can visit the Sir M. Visvesvaraya Museum and learn about his life and contributions.

5.Bangalore: Bangalore, the capital city of Karnataka, is located about 25 km from Dodda Hoskote Lake. The city is known for its vibrant culture, beautiful parks, and historical landmarks. Visitors can explore popular tourist attractions like the Bangalore Palace, Lalbagh Botanical Gardens, and the Vidhana Soudha.

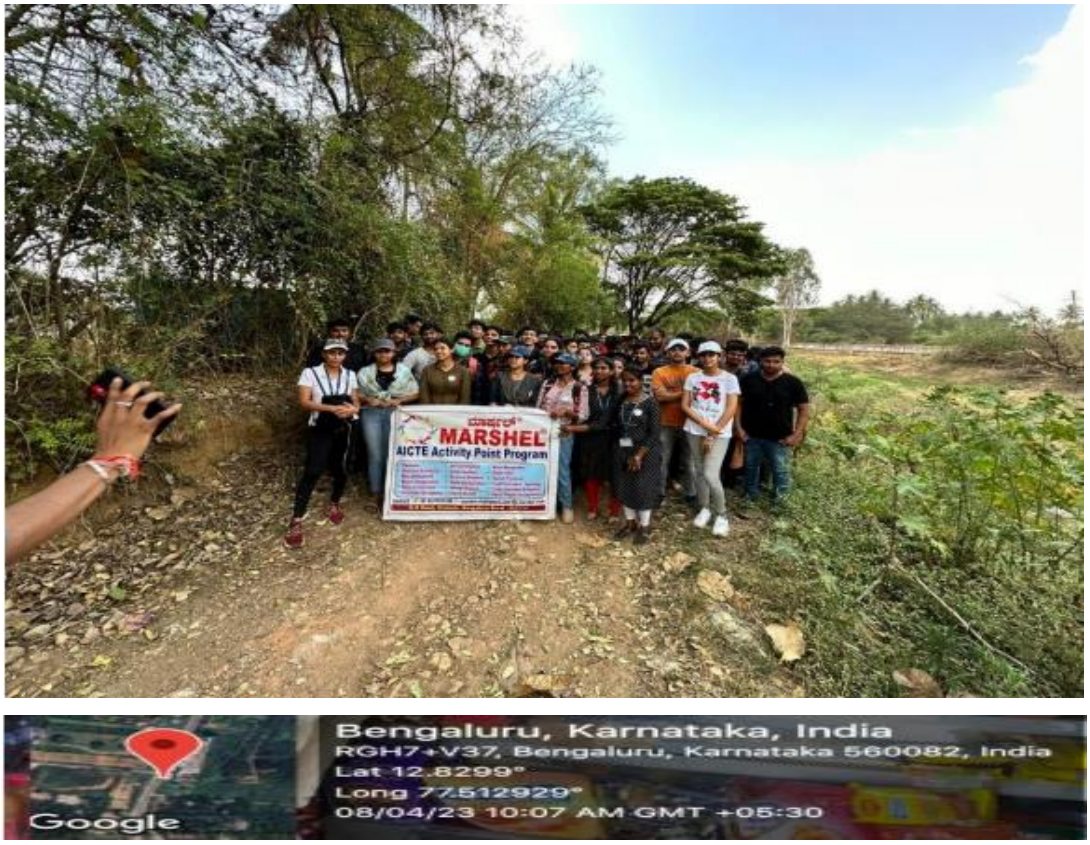


Fig 3.1 : Near Dodda Hoskote Lake

3.3 OUTCOME OF THE ACTIVITY

Some of the points regarding Tourism are given below:

1.Tourism is an important industry: Tourism is a significant source of revenue and employment for many countries and communities worldwide.

2.Types of tourism: There are many different types of tourism, including leisure tourism, business tourism, adventure tourism, cultural tourism, and medical tourism.

3.Positive impacts of tourism: Tourism can have many positive impacts, such as boosting local economies, preserving cultural and natural resources, and promoting cultural exchange.

4.Negative impacts of tourism: However, tourism can also have negative impacts, such as environmental degradation, cultural erosion, and crowding.

5.Sustainable tourism: To address these negative impacts, sustainable tourism practices have been developed to minimize the negative effects of tourism while maximizing the positive ones.

6.Technology and tourism: Technology has played a significant role in the tourism industry, from online booking and virtual tours to the use of big data and artificial intelligence to improve the tourist experience.

7.Tourism and COVID-19: The COVID-19 pandemic has had a significant impact on the tourism industry, with travel restrictions and reduced demand leading to a decline in tourism activity.

Fig 3.2 : Dodda Hoskote Lake

CHAPTER 4

SETTING OF THE INFORMATION IMPARTING CLUB FOR WOMEN LEADING TO CONTRIBUTION IN SOCIAL AND ECONOMIC ISSUES

CYBER SAFE

Duration:80 hrs(27 Nov 22 to 10 Dec 22)

This course contains 50 chapters:

Chapter 4.1

MOBILE RECHARGE SHOP

If you want to recharge your mobile phone, which is the place that you would go - a local mobile recharge shop near your house or by the customer care of the mobile service provider? Ideally, most of us would say the former one as it is more convenient. Did you know that this could be a potential source of being a victim of cybercrime?

It is like giving off your personal information like phone number as well as ID proofs to a complete stranger. The stranger can send an SMS to your phone asking you to click on a link or scan a QR code which may result in money being debited from your account or in worse cases even your phone being hacked. being installed. The ID proof submitted to them might be used to create a fake identity in your name and can put you into trouble for something that isn't your fault at all. The mobile recharge shop vendor who seemed extremely nice to you at the beginning over text could even manipulate you eventually. Hence being aware and not recharging your mobile with local recharge vendors would save you from a lot of trouble and help you stay safe.

Chapter 4.2

DEBIT CARD CLONING

We swipe our credit and debit cards at shopping malls, petrol bunks, ATM's etc, little do we realise to check the swiping device for any extra parts attached before swiping our cards. These swiping machines may be fitted with an extra skimming device that reads your card details and your PIN and then the scamsters who inserted the device may use it for fraudulent transactions.

The scamster may even be able to replicate the card and withdraw money from an ATM with the help of your card details and PIN that was obtained by the skimming device. Making sure that no one is peeping while you are entering your pin, as well as not sharing your PIN with anyone (including your friends) is a good practice to avoid being a victim of a fraudulent transaction. So the next time you step into an ATM, look around for spy cameras, check the place where you insert your card to check for any movable parts or extra fittings and if there is a pad over the keypad to capture your PIN. Be attentive, be careful and save your money from being transferred into the hand of scamsters.

Chapter 4.3

KEYLOGGER

Keyloggers are generally malicious programs or devices that are used by a hacker or scamster to capture your keystrokes. Which essentially means that if a keylogger is installed on the victim's machine, the hacker can see the websites you visit, the passwords you type, the photos you view, your financial card details and even enable your webcam and microphone. Hence the hacker knows every move that you make on your system and this can be quite scary. The pictures taken by the hacker may be used to blackmail or even manipulate you.

Keeping your laptop or phone updated with the latest software is extremely important and might even prevent such incidents from happening in the future. Also, make sure that you have antivirus in your systems which can scan for such keyloggers. Before using an ATM or entering your PIN make sure that you aren't typing on any sort of pad coating instead of the keypad directly. Not leaving your unlocked laptops unattended and making sure you have a password for your device are also important steps to be taken to prevent your keystrokes from being captured by a stranger

Chapter 4.4

SMS SPOOFING

Spoofing is essentially deceiving the receiver of the sender's id and number. So the sender pretends to be someone else just in order to get the user to click on a malicious link or to gain personal information of the receiver. A spoofed SMS is sent from the fraudster's phone to the victim in order to entice the victim. The victim unaware of this type of cybercrimes might think it is genuine and since the sender's name matches whom the sender pretends to be, the innocent victim is easily convinced.Watch out for such SMS's that say you have an unreasonably huge sum of money or a free trip to a country on your bucket list. It is coming from a fraudster and you might just end up losing money or giving away your personal information only to be blackmailed later on. Beware and do not click on unnecessary links or even reply to any SMS from an unknown person. Remember that nothing comes free not even a toy car, so forget about winning 1 million dollars.

Chapter 4.5

CALL SPOOFING

Spoofing means to pretend to be someone that you actually are not. Fraudsters call people promising job interviews in their desired companies or saying they are interested in the product that you recently wanted to sell on a website. After a convincing conversation, people believe the fraudster who tells them to scan a QR code and in a few seconds, you notice that money has been debited from your account. There are incidents where the scamster pretends to be one of your friend in trouble and even changes his voice to make you believe it.

There are certain easily available apps that allow the scamster to change their number in order to conduct call spoofing. Hence be careful and do not give away any of your personal details to anyone whom you do not trust over a call. Never share OTP's or your debit card PIN's with anyone. Having an app that shows the caller ID or suggests that it might be spam might also help against being a victim of spoofed calls.

Chapter 4.6

RANSOMWARE

Ransomware is a type of malware that encrypts your files and you need to either restore it from the latest backup that you have or pay the hacker in order to obtain the encryption key in order to access your files. About 50 percent of the time, even after paying the hacker the demanded amount, you might not get your files back. Also if your files contain sensitive customer information, such details will be exposed to the hacker which can ruin the reputation of your company.

Phishing emails are one of the most common ways for ransomware to infect your network. Hence employees of the company must be trained and made aware to avoid clicking unnecessary links in emails or downloading attachments. Keeping your antivirus and operating system updated may also help prevent your systems from getting infected with ransomware.

Chapter 4.7

CYBER STALKING

Cyberstalking is using the Internet to stalk or harass someone based on the information on their social media accounts. Letting people know where you are at a given point of time, the restaurants you are visiting etc. gives people more information about you. Keeping your social media accounts public lets even strangers know about your family, friends, common places you visit and sometimes even where you stay. This means that a person with a wrong intention may even follow you home since they know where you stay through the information that you have shared on social media.

Be careful with the friends you make on social media. Think before you post personal information or even your current location on the Internet. Accept only requests from the people you know and preferably ensure to keep your profile private. Be careful and stay safe.

Chapter 4.8

PICTURE MORPHING

Morphing the face of one person to the body of another person and publishing it online in order to blackmail the victim is called picture morphing. This is often done as an act of revenge by a previous acquaintance or by a complete stranger. Sharing pictures with a person you recently made friends with on social media is hence not safe as he could misuse those pictures. Make sure to keep your profile private and accept friends requests from only the people you know.

While uploading pictures on the Internet, make sure they are not clear images as they can be easily morphed. Hackers do not need expensive tools to morph pictures. It can be done easily with the click of a button, hence think twice before sharing pictures on social media. Personal information like phone number should be considered twice before uploading it on your social media accounts.

Chapter 4.9
PROFILE HACKING

Keeping a watch on the kind of games your children or little ones are playing is soo important in this current generation. Most of the kids download and play the games without knowing the consequence it has on their body and mind. Especially for kids and teenagers who are more likely to get depression and have low self-esteem may harm themselves while playing such toxic games. This may become addictive overtime and even may lead to killing oneself in the worst cases.

Hence it is important as adults to keep a watch and completely know what type of games the kids and teenagers are downloading and playing. Also if behavioural changes are noticed in kids after playing certain online games, then that must be treated properly and must be advised accordingly.

Chapter 4.10
ONLINE GAMES

An email account or social media account being hacked by a hacker is called Profile Hacking. Forgetting to log out of your accounts on public computers might enable the next person using the system to reset the password of your account and hence hack your account. Hence

logging out of all public computers is extremely important to protect your account from being hacked.

Also accessing your email and social media accounts when you are connected to a free Wifi at restaurants, airports, or public places might make it easy for a person to capture your passwords and hence it must be avoided.

While setting passwords of your social media accounts it is important to choose a strong password and not reuse the same password across all accounts. Make sure not to share your passwords with other people. Logging out of all accounts and enabling two-factor authentication might also help prevent your social media account from being hacked.

Chapter 4.11

JOB CALL LETTER

While you are in search of a job, you upload your contact details on multiple websites that say that they will help you find a job. During such desperate times, none of us actually put in the effort to check whether the website is genuine before we apply on it. This is one extremely crucial step that we miss and hence we may be a victim to a fake job offer. Often calls are also received from several agencies promising to give you the opportunity of attending an interview at your dream company in return for a few thousand.

Websites offering jobs must be checked for its authenticity and mails received from the companies you apply to must be checked before going for an interview. All you know it might just be a phishing mail. Remember that even though you register on websites offering jobs, none of them nor the companies you apply to require you to pay any money. It is also important to verify the details of the company that you are going to interview for, before going for the interview in order to make sure it is genuine.

Chapter 4.12

DEEPFAKES

Deepfake is basically a technology to combine and superimpose new images and videos onto source images and videos. This is done in such a way that the viewer cannot doubt the truthfulness of it. Deepfakes are generally done by people who have some technical knowledge as it uses artificial intelligence in order to superimpose the images or voice. This

can be used to manipulate or blackmail an innocent victim.Hence it is important to not upload your clear photos and videos on any social media platform. People with wrong intentions can use those pictures itself to create a deepfake and make it viral to bring down your reputation. Since deepfakes use some amount of technical knowledge in order to create it, hence it looks as close to real as possible.

Chapter 4.13

DATING WEBSITE

Girls are often emotionally manipulated by people who seem to be extremely nice at the beginning but might actually just want to take advantage later on. Dating websites are one such platform which has made this easier online. Girls trust the person they just started texting on a dating website and share all personal information as well as pictures with them without even getting to know them properly. Sometimes if the boy even asks for a lot of money, the girl lends money without even thinking twice and this transaction might turn out to be their last conversation if the guy turns out to be a scamster instead.

Hence, girls must be extremely careful when they are using such dating websites. It is important to not trust the person blindly but instead to get to know all details about the person they just met on the dating site before trusting him. Be careful while sharing private pictures and videos and stay alert and stay safe.

Chapter 4.14

CAMERA HACKING

Girls are often emotionally manipulated by people who seem to be extremely nice at the beginning but might actually just want to take advantage later on. Dating websites are one such platform which has made this easier online. Girls trust the person they just started texting on a dating website and share all personal information as well as pictures with them without even getting to know them properly. Sometimes if the boy even asks for a lot of money, the girl lends money without even thinking twice and this transaction might turn out to be their last conversation if the guy turns out to be a scamster instead.

Hence, girls must be extremely careful when they are using such dating websites. It is

important to not trust the person blindly but instead to get to know all details about the person they just met on the dating site before trusting him. Be careful while sharing private pictures and videos and stay alert and stay safe.

Chapter 4.15
SOCIAL TROLLING

With this current era where most people are on social media, a lot of hate is spreading among people through social media. One such incident is social trolling, which basically means making fun or posting inflammatory comments and posts in order to just cause a nuisance to a person. People do not consider this to be a huge cybercrime but it affects a lot of people's mental health. People who are vulnerable to clinical depression or having low self-esteem might get severely affected by such comments and posts.

The victim also loses her reputation and gets more scared to talk to her parents about this. Most of such cases are just ignored or the victim thinks it is okay to suffer through it. Although, it is extremely important to inform adults or even lodge a complaint in the police station if it is a severe case.

Chapter 4.16
PONZI SCHEME

A Ponzi Scheme is a fraudulent investment scheme that promises high rates of return with little risk to investors. Afterall somethings are too good to be true. Victims who believe in such schemes are vulnerable to hackers who promise to recover their loses. When you have already lost money in a particular investment scheme, you want to the money somehow without even thinking about checking the truthfulness of the hacker. Hence, making decisions in a haste might not be the right way.

Always check the right schemes and something that is more realistic before investing. Even if after all that you have done, you get cheated on, take time and check the truthfulness of anyone who says that they will return your money back. Stay safe and let us hope you do not get tricked twice.

Chapter 4.17

FAKE MATRIMONIAL PROFILE

A fraudster who has registered on a matrimonial site with his fake profile might start texting a girl and eventually make a girl fall for him. The profile photo and details may not even be his since it is a fake profile. The girl however believes and trusts this person and assumes he is the person who he is pretending to be. During his difficult times, she may even give me some lakhs of rupees and then the man might disappear after receiving the money. This is when the girl releases that it is a fake profile but by then it is already too late.

Such kind of fraudsters exists, who cheat on multiple such women with the same modus operandi. Hence being aware and doing some background verifications too while you meet people on matrimonial sites goes a long way and might help prevent being cheated by people having fake matrimonial profiles.

Chapter 4.18

MOBILE REPAIR SHOP

Do you go to the official store if your mobile doesn't work or do you go to any mobile repair shop close to your house? The latter is where the risk arises. In case you go to the mobile repair shop and drop off your phone telling the vendor that you will collect it in a while, then he has access to all your photos, videos, messages and contacts. Is locking your phone with a pattern or passcode enough to prevent him from accessing this personal information? Certainly not, since the patterns and passcodes can be easily cracked with the help of hacking software.

Furthermore, those pictures can be used to blackmail the victim. Hence it is important to get the phone repaired at the official store itself instead of a local repair shop. Also preferably it is better to wait till your phone gets repaired than leaving it with him itself. Be careful and stay safe

Chapter 4.19

FAKE REVIEWS

Fake reviews are least realised in any product on any website. Some products might have fake reviews just in order to increase the sales of that product. Hence they trick customers into buying that particular product. Sometimes these wonderful reviews are backed by exciting discounts and offers in order to entice the customers even more. At times such products may even cause untold harm if used.

Hence before you buy a product, buy from a genuine website and look at the genuine reviews. A lot of browsers allow you to install extensions that might help identify fake reviews. Also, look at the total number of reviews while checking out the percentages of reviewers who liked the product. Keep your skin safe and trust only websites and products that show genuine reviews.

Chapter 4.20
FAKE PROFILE WITH SEXTORTION

Any public changing rooms or public washrooms might have cameras placed to capture pictures with criminal intent. These pictures are later uploaded on fake social media profile with the intention of extortion. The helpless innocent victims end up paying huge sums of money for that to be removed from social media and for no fault of theirs. But by that time it would have already been sent to the victim's family and friends.

Hence it is important to check for any spy cameras in any public changing rooms or washrooms. Also, check for 2-way mirrors and report any sort of blackmailing to the police officials at the earliest. Stay safe and report it at the earliest.

Chapter 4.21
CYBER VULTURES

An organisation or person has currently just faced a cyber attack and these hackers again try to attack them, These merciless breed of hackers are called cyber vultures. They make use of the desperate state of mind of such people and try to swindle more money from them. Hackers call and convince you that they are genuine and that you will get your money back and hence manage to obtain the sensitive information like UPI code, ATM PIN etc. With this information he debits more money from the account, adding to much more damage.

Amounts received in such transactions might be transferred to an unknown E-wallet company which refuses to comply with investigation agencies.

Hence, it is important to be sure of random callers and never share your OTP or PIN with anyone. Also, verify the authenticity of the person or organisation who is trying to help you after a cyber attack. Firstly, try not to be a victim of a cyber attack in the first place and even if you become, do not succumb to another attack. Stay aware and stay safe.

Chapter 4.22

APP TRAPS

Before downloading any app onto your phone it is extremely important to know what exactly the app does. Some apps are known to just harvest data from your phone and transfer it to some person/organisation. These apps might request access to your storage, files, pictures, camera etc. and once you grant them the required permission, they can see all your photos, videos, sensitive documents and even capture photos and videos of you without your knowledge. The companies of such apps also sell your data and make a huge amount of money by this method.

Therefore, it is important to always download apps from google play store and not from APK's available online. Also, give permissions only as required. If an app does not actually make use of a camera , then you need not give it such permissions. Be aware of all the apps you have on your phone and make sure you know what each of them do. Be safe.

Chapter 4.23

JUICE JACKING

Have you charged your phone from public charging points like in airports, restaurants and malls? Have you ever wondered if it safe to charge from those sockets? Indeed, it might not be safe at all. Some charging ports might install malware or copy sensitive information from your phone or any other device. This especially happens in charging ports that doubles as a data connection, most likely over USB. In case you observe your phone becoming slower or hotter suddenly, and if you have been charging your phone at any public charging points, your phone might have some malware installed on it. Doing an antivirus scan will show the presence of malware and that is causing the reduction in speed and hence it is important to

have an up to date antivirus. Think twice the next time your phone has a low battery and you want to charge it at a public charging point.

Chapter 4.24

WIFI HACKING

WiFi is a wireless technology that lets laptops, smartphones, smart TV's etc. connect to it in order to be connected to the Internet. Most homes and offices nowadays have a WiFi with multiple devices connected to it. When your house gets a WiFi it comes with a default password and most of the times it remains unchanged. WiFi hacking is essentially cracking the password of your WiFi. If your neighbour wants to use your WiFi, he might just try the default password that you haven't changed yet and directly start using your WiFi. Do not be surprised if you get a huge bill or notice that your internet speed has decreased.

Keeping weak passwords lets hackers get connected to your WiFi and then can view, store, download or abuse your network. Also, people with bad intensions can connect to your WiFi and commit crimes like sell drugs etc. which causes trouble for no fault of yours. Hence, it is important to keep a strong WiFi password and have a check at the people logged onto your WiFi frequently.

Chapter 4.25

ONLINE RADICALIZATION

A lot of teenagers and young adults might fall prey to online radicalization or terrorist's propoganda while surfing the internet. The extremists target individuals who are weak minded or currently going through financial difficulties in their life. They lure them with some amount of money and inculcate terrorist ideologies in their mind. Such gullible people often fall prey to such forms of online radicalization because of either a weak upbringing or past experiences.

The mind can be easily manipulated and hence it is important to not blindly believe anything. Check the facts and check if this is the thing that you believe in and are not forced in endorsing it because of external pressure. Question your integrity and morality before trying to believe or do as the extremists say. Have your own ideologies and stay strong and stay safe.

Chapter 4.26

HONEY TRAP

Honey is always sweet but as they say life is not always sweet. Honey trapping is using romantic or intimate relationships just for an interpersonal, political and monetary purpose. Girls trust men who compliments them and gets close to them in sometime. Little do you know that the person might have an hidden motive behind it. He might just want some money from you or some sensitive information. Once his motive is achieved, he will no longer contact you or keep in touch.

Hence, once you become friends on the Internet, it is important to do a background check and get to know a person properly before trusting him directly. Also they may use your pictures or videos and then may later blackmail you just in order to get some money. In this current era, with the increased use of social media platforms, it makes it easier for people to blackmail

Chapter 4.27

QR CODE SCAM

QR code is a 2 dimensional barcode which was initially used to make it easier for people to search websites. Just one scan of the QR code would take you to the exact URL that you are interested in instead of typing the entire URL in the search bar. But however nowadays, this is being misused as any URL can be embedded in a QR code. Half the payments that are done on a daily basis happen by just scanning QR codes these days. QR codes are sent by scamsters to innocent people and they tell them to scan their code and within seconds money gets debited from their account.

Hence it is important to remember not to scan any QR code unnecessarily. Also since all QR codes look the same you might never know what the real intention behind the QR code is. Therefore if it is someone you do not trust, it is always better to enter the URL by yourself itself. Your phone can also get hacked by just scanning a QR code, so be careful.

Chapter 4.28

RFID CLONING

RFID refers to Radio Frequency Identification which is a method of automatic authentication of objects and object ID's using radio waves. Each RFID chip contains an identifier which consists of a unique number and an antennae. Hence most RFID cards can be easily cloned.

It is important to not leave your RFID cards unattended as someone might get an RFID card reader and scan your RFID thereby obtaining all details. It therefore can be easily replicated and can be used to gain access to all the things you have access to with that RFID card.RFID cards are mainly used in offices as an access card to some of the most confidential rooms like server rooms and only limited people have access to it. Hence if your RFID gets cloned someone else might have access to it and if anything is tampered then you might be blamed for it with no fault of yours.

Chapter 4.29

DRONE SURVEILLANCE

A drone refers to an unpiloted aircraft. Drones are used for a variety of purposes like detecting cracks on railway tracks, delivery of medicines and goods , to take videos and pictures etc. Drones typically have a camera fixed to them in order to capture images and videos during the day as well as in the night. Even though drones are extremely useful for a lot of purposes, they can be misused as well. They maybe able to intercept cell phone calls, determine GPS locations, gather license plate information, and go even where a human can physically not step in.

People can hover drones outside your bedroom and take pictures of you without your knowledge. They can also intercept and crack your WiFi password as well as drop some hazardous weapons. A CCTV camera with a motion sensor maybe helpful in detecting a drone and could help prevent such an incident from occuring.

Chapter 4.30

SEARCH ENGINE RESULTS SCAM

All that you search on Google may not be actually genuine websites. Hackers can create a legitimate looking website and make it appear in your search results. Since it appears in your results, you might assume that it actually is genuine and hence might view the website.

However a lot of your results might just be to mislead you. Do not trust any customer care or helpline number that you come across on your seach result. It might just be a fake number and you might end up giving away your personal information to an unknown person, or in worse cases even end up giving money to the wrong person.

This Search Engine Optimization scam can trick a lot of users and hence it is important to check the authenticity of a site or helpline number before falling prey to one of them. Beware and do not share your CVV with anyone or give out any personal information to a complete stranger. Do not see and blindly believe without verifying the truthfulness.

Chapter 4.31
IDN HOMOGRAPH ATTACK

The internationalized domain name (IDN) homograph attack is used to form domain names that visually resemble legitimate domain names, albeit, using a different set of characters. For example, the IDN "xn--akmai-yqa.com" which appears in unicode as "akámai.com" visually resembles the legitimate domain name "akamai.com". Attackers often apply IDN homograph attacks to form domain names that are used for malicious purposes, such as malware distribution or phishing, while appearing trustworthy to victims.

An IDN homograph attack is similar to another type of domain name spoofing known as typosquatting. Both techniques attempt to deceive users by using a new domain name that's similar to an established name, although they exploit different types of similarities. Typosquatting uses a new domain name that's spelled differently from the established name, but uses the same character set. A homograph attack typically uses a domain name that contains characters from other character sets, which requires the user to click on a hyperlink of the new name. This type of attack rarely works with a manual entry of the domain name since a user is unlikely to unintentionally enter a homograph.

Some domain names can be used for both typosquatting and homograph spoofing. For example, a spoof that uses a domain name containing an uppercase "O" instead of the numeral "0" would be both types of attack. The success of this type of spoof is highly dependent on the typeface the computer uses, as these two characters are physically identical in some typefaces.

Chapter 4.32

SCRATCH CARD SCAM

There are a variety of fraudulent or deceptive schemes prevalent online, where people are asked to make payments/ share account details or OTP/participate in money multiplying schemes etc. via email, phone or text. Fraudsters use many methods to conduct scams, including requesting gift cards from well-known brands for payment.

While the specifics of the scams vary, scammers generally follow a common pattern: they connect with a victim by phone, email, through social media, or online; they create a sense of urgency (for example: by offering a great price or mentioning a personal hardship or emergency); they ask for payment using gift cards; and they instruct the victim to purchase gift cards online. The scammer then demands or instructs the victim to provide the email with a claim code on the gift card by phone, text message, or email - and then disappears.

Chapter 4.33

SIM SWAP

SIM swap fraud is an account takeover scam that targets a weakness in some forms of two-factor authentication in which a call or text message sent to a mobile telephone is the second factor or step. Also known as port-out scam, digital SIM swap, SIM splitting, and simjacking, the SIM swap scam exploits the ability of subscriber identity module (SIM) cards to be ported seamlessly by mobile phone service providers from device to device bearing different telephone numbers. Typically, carriers use this feature when customers buy new phones, switch service, lose their device, or experience theft.

At its most basic level, during a SIM swap, a SIM hijacker convinces your mobile carrier to port your phone number over to their SIM card. By transferring those incoming messages, fraudsters can easily access your most sensitive accounts by completing text-based two-factor authentication checks. If you've failed to protect accounts with 2FA, they can use the phone number to generate existing and new passwords. They can also take over social media accounts, retail accounts, and any other accounts linked to the phone number—which is probably any online account.

The primary goal of SIM swap fraud is typically financial gain, often in the form of stealing bank and credit card information. However, sometimes a SIM swap attack might be intended to embarrass or humiliate the victim when compromising social media accounts.

Chapter 4.34
CRYPTOJACKING

Cryptojacking is the unauthorized use of someone else's computer to mine cryptocurrency. Hackers do this by either getting the victim to click on a malicious link in an email that loads cryptomining code on the computer, or by infecting a website or online ad with JavaScript code that auto-executes once loaded in the victim's browser.

To produce new blocks, cryptocurrencies rely on individuals to provide the computing power. Cryptocurrencies reward people who supply the computing power with cryptocurrency. Those who trade computing resources for currency are called "miners".The larger cryptocurrencies use teams of miners running dedicated computer rigs to complete the necessary mathematical calculations. This activity requires a significant amount of electricity – for example, the Bitcoin network currently uses more than 73TWh of energy per year.

Hackers have two primary ways to get a victim's computer to secretly mine cryptocurrencies. One is to trick victims into loading cryptomining code onto their computers. This is done through phishing-like tactics: Victims receive a legitimate-looking email that encourages them to click on a link. The link runs code that places the cryptomining script on the computer. The script then runs in the background as the victim works.

The other method is to inject a script on a website or an ad that is delivered to multiple websites. Once victims visit the website or the infected ad pops up in their browsers, the script automatically executes. No code is stored on the victims' computers. Whichever method is used, the code runs complex mathematical problems on the victims' computers and sends the results to a server that the hacker controls.

Chapter 4.35
VIDEO CONFERENCE SCAM

Also called as Zoombombing is a type of cyber-harassment in which an individual or a group of unwanted and uninvited users interrupt online meetings over the Zoom video conference app. This disruption occurs when intruders gate-crash gatherings -- sometimes for malicious purposes, such as sharing pornographic or hate images or shouting offensive language -- without the hosts permission.

Conferences are vulnerable to Zoombombing when they are hosted on public channels shared over the internet through URLs, making them easily accessible to unwanted trolling. Hijackers can sometimes figure out the correct URL or meeting ID for a public Zoom session and gain access to the meeting. A basic Google search for URLs containing "Zoom.us" can unearth unprotected links of meetings; plus, links to public meetings may be available on organizational pages on social media.

In addition, if Zoom screen-sharing privileges are not set to "host only," uninvited guests can share disturbing images or potentially malware. Also, a remote-control feature lets users take control of another participants screen in a meeting. A user can either ask for remote control of another participants screen, or the other participant can grant control to a user.

Chapter 4.36
KIDS MOBILE PHONE

Due to the ongoing trend of playing online games, children insist on getting their own mobile or play online games using their parent’s phone. In these games, to enter the next level or to buy an avatar, weapon or dress, an online payment has to be made, which kids often make through their parent’s online banking or debit/credit card without informing them. Later on, the parents complain to the police about the online financial fraud

Chapter 4.37
SMART HOMES

As hot new gadgets seek to make your home smarter and more efficient, it’s still up to you to learn how to secure the connected devices throughout your smart home.Your internet-connected devices — smart TVs, security cameras, smart locks, gaming consoles, smart thermostats — can add a level of convenience to your life, but they could also make your home and connected devices vulnerable. That’s why it’s important to have a defense plan

for securing smart home devices.The Internet of Things — all those appliances and devices that connect to the internet and to each other on your home network — have created new opportunities for cybercriminals.

Bottom line: If you have a connected home, it needs protection.

Internet of Things devices — IoT devices, for short — can offer new points of entry for cybercriminals.

Cybercriminals have hijacked baby monitors and spied on people using their webcams, for instance. If you own a smart home device, your privacy and security could be at stake.

No one wants a hacker to infiltrate their IoT network. Consider a few scenarios.

What if a cybercriminal accesses data on your smart thermostat to figure out when you're home or away?
What if a hacker gets into your network through an IoT device for a ransomware attack. A ransom could be demanded to get your system working again, with no assurance the cybercriminal will actually restore your access.
What if someone accesses information you've shared with your digital assistant — those voice-activated speakers such as Amazon Echo or Google Home? Maybe you shared passwords or financial information. It could be exposed.
That raises security issues.

Home routers and security cameras are top IoT targets for hackers. Why? Because — like most other connected devices — they have little or no built-in security. That makes them vulnerable to malware.

And there's another reason. Security usually isn't a top priority for IoT device makers. Their poor security practices could include these:

No system hardening, which gives a computer system various means of protection and makes it more secure.

No mechanism for updating software, which can create vulnerabilities.
Default or hardcoded passwords, which hackers can exploit.

No doubt more IoT devices are coming and will angle for a place in your home. If they make your life more convenient — even happier — great. But don't forget to secure your increasingly smart home and your IoT devices.

Chapter 4.38
MICRO LOAN

Loan sharks are now attacking digital ecosystems by promising instant money to people who are running from pillar to post in the aftermath of the pandemic which has decimated businesses and rendered millions jobless around the globe.A loan shark is a person who – or an entity that – loans money at extremely high interest rates and often uses threats of violence to collect debts. The interest rates are generally well above an established legal rate, and often loan sharks are members of organized crime groups.

Loan sharks do not require background checks or credit reports. They will lend large sums of money with the intention of gaining high levels of interest in a short time. Loans from loan sharks charge interest rates far above any regulated rate. For example, a loan shark might lend Rs10,000 to a person with the provision that Rs20,000 be repaid within 30 days. These lenders may also often call on the debt to be repaid at any time, using violence as a means of forcing repayment.

A lending app will always ask for your permission and share the details of the action it desires to take with your data. Your smartphone is a storehouse of your personal details, pictures and other sensitive information. Do take a minute to review the kind of permission you are granting.The perils of online fraud are unlimited. Whether you are exposed to an online scam or locate one, file a complaint on www.cybercrime.gov.in or visit the nearest cyber crime police station.

Chapter 4.39
BLUE SNARFING

Bluesnarfing is a type of network attack in which an attacker gains unauthorized access to a wireless device via a Bluetooth connection. Once the hacker has access to the device, they can steal sensitive user information, including personal photos, contact lists, emails, and passwords. Below are several ways you can prevent a Bluesnarfing attack.

Cybercriminals can perform the bluesnarfing attack on a device even when it is more than 100 feet away. What they can steal by doing so is mindblowing and quite scary. They can practically copy the entire content of your phone or device, including your emails, contact list, phone number, passwords, and your pictures. Some bluesnarfing attackers use the victim's phone to call long distance, leaving its owner with a huge telephone bill. All these happen without the victim's knowledge, of course, and so attacks can go on for a long time.

To understand how bluesnarfing is done, it's important to first know how Bluetooth works. Devices that are Bluetooth-capable communicate with each other using the so-called Object Exchange (OBEX) protocol.

The OBEX protocol has inherent security vulnerabilities that attackers can exploit using tools such as Bluediving. With it, attackers can look for Bluetooth-enabled devices and pair with these without their owners' knowledge.
If they have programming skills, the attackers can create their own bluesnarfing tool. However, even those who don't know how to code can still use bluesnarfing to steal data. There are ready-to-use attack tools available online. There are also bluesnarfer-for-hire services that they can employ.Any form of theft is scary, and these days, digital theft is alarmingly rampant. Bluesnarfing is just one of the many methods by which attackers can steal your sensitive and confidential data.

Chapter 4.40

STOLEN PHONE

Smartphones have become our indispensable companions—our best buddies for doing everything from playing games to getting around to keeping in touch with friends and family. But how much personal data are you sharing about yourself along the way? What happens if our phone is stolen?

Having your phone stolen is a frustrating and difficult experience. Whether you're at home or traveling abroad somewhere, it's important that you try as soon as possible to recover the stolen phone. Current cell phones and smartphones can be recovered through the use of a tracking app, or by a pre-installed tracking program. These apps and programs have varying levels of practicality, and some require your phone to be on and connected to the internet. You can also find a missing phone manually, by calling or texting the number and retracing your steps.

The average smartphone user these days has between 60 and 90 apps on their device. Most of these apps request some sort of information about you and the device you are using. They may want to know your name, your email address, or your real-world address. But because smartphones are so powerful, they can also get quite a bit more than that, such as your exact location. Some apps will even request access to the device's camera or microphone.

All the applications and the internet sites you're accessing daily collect the essential information about you in order to create your digital ID profile. All of this information that has been collected by applications is developed with a single purpose; to improve the user experience, or so that is what the larger companies want us to believe. Your smartphone is overloaded with information about you – intimate conversations, health records, financial data and your most recent visited locations.

So your phone is basically a treasure house of your data! Therefore it is important to ensure the data doesnt get misused/leaked when the phone is stolen/lost.

If you've determined that your phone isn't just temporarily misplaced, it's wise to take more advanced steps to protect your information and identity.

1. Report the loss to your cell phone carrier immediately
2. Remotely lock and wipe your phone if possible
4. Change your passwords

Smartphone companies often offer cloud services, allowing your phone to access your data in the cloud. To prevent the thief from doing so, you'll want to change your cloud password as soon as possible. You should also change your passwords for any other accounts that you access on your phone, such as banking, social media, email, and other accounts.

As the old saying goes, "An ounce of prevention is worth a pound of cure," and in this

particular case, it has never rung so true. Follow the tips mentioned at the end of this chapter to help you protect your phone and your information if you ever lose your phone.

Chapter 4.41

EXAM MALPRACTICE

Exams are something which we all hate and want to avoid but why are exams existing anyways?

• Examination is very important in every person's life. Examination tells us our goodness's and shortcomings. It tells us our mistakes and corrects them and helps us to move forward. Through examination, we get to know where we are behind and we can move ahead of improvement. If we succeed in the exam then move on and fail then we get experience and learn something new which we always remember. Examination enhances our personality and knowledge.

• If the exam will not be conducted from time to time, then we will never be able to donate our mistake and learn anything new. We have a lot to learn from either success or failure in the exam. If we are successful, we go to a new stage and if we fail, we get many experiences which are useful to us throughout our life. Without examination, we can never know our own shortcomings. Exams explain us about life and lead us through learning something good.

• Often student who have exams undergo severe pressure,stress,anxiety or depression.

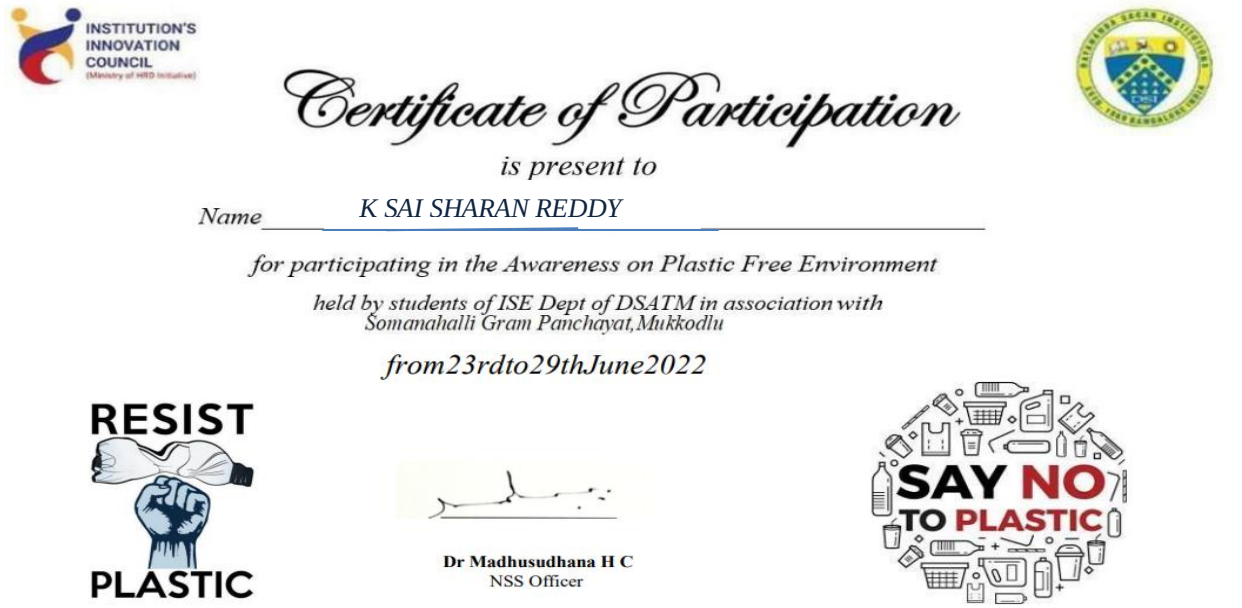
• Every time we hear about a student committing suicide in India, we assume failure in some exams to be the cause. Students preparing for exams often feel under pressure. The pressure may result in feelings of anxiety or nervousness, and this exam stress can interfere with the individual's daily life. While a certain amount of stress may be beneficial, too much exam stress can cause individuals to perform poorly on tests that mean so much to them.

• There several reasons why students fail in their exams like:

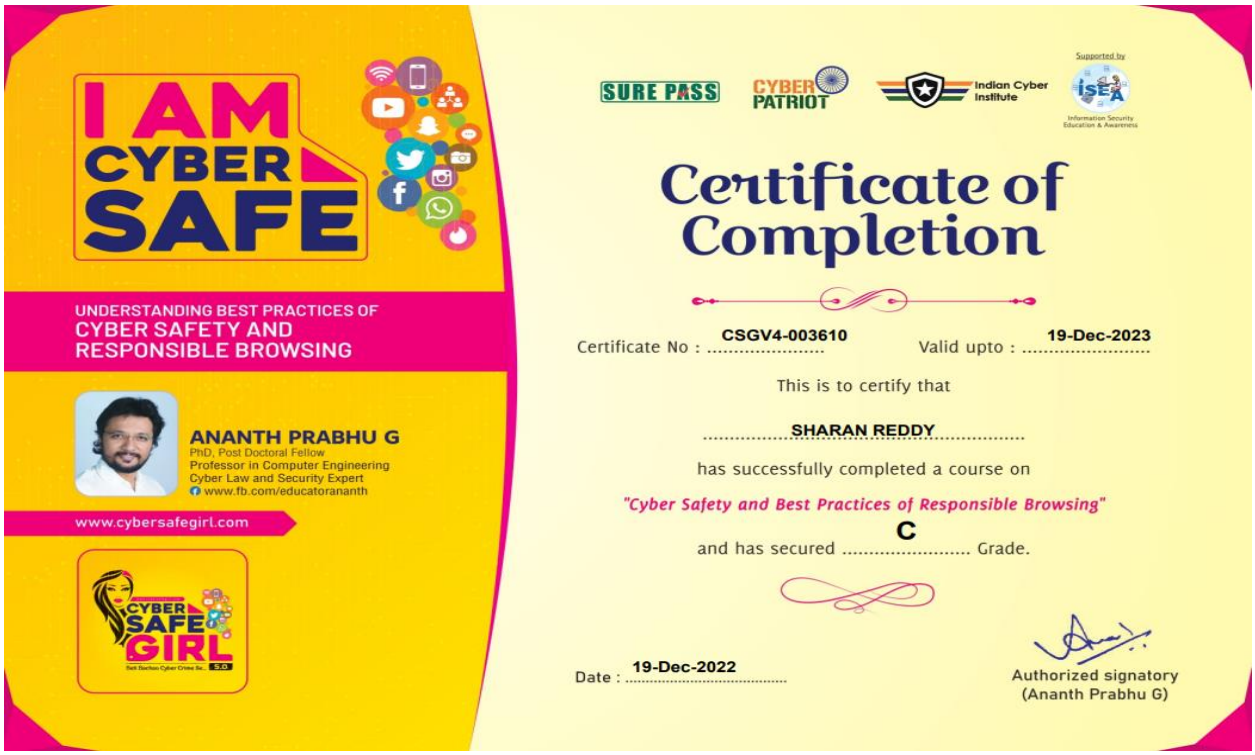
• Not have studied enough, they may find the material difficult, or perhaps they feel tired because

CERTIFICATES

Plastic free Awareness Program



Cyber safe girl



Swachh Bharat (Greenathon)