



ZINDAGI
TRUST



DIGITAL حفاظت

Guidelines for Children







Zindagi Trust, TikTok and Pakistan Telecommunication Authority have come together to create a valuable guide for children, parents, and teachers, centered around Internet safety. This collaborative initiative aims to provide essential knowledge and support, fostering a protected online experience for individuals of all users specifically children. Its primary objective is to ensure a secure online environment. Through this partnership, potential risks and challenges are addressed, and individuals are empowered with the necessary knowledge and tools to navigate the digital world safely and responsibly.

This book represents a comprehensive and invaluable resource, equipping readers with the knowledge and tools needed to navigate the internet securely. With a strong emphasis on Digital Safety, it offers practical tips, actionable advice, and insightful perspectives to help readers understand and effectively mitigate potential risks. By empowering individuals with this information, we strive to create a safer and more responsible online community for everyone involved.



**ZINDAGI
TRUST**



**Ministry of Information Technology &
Telecommunication**
Government of Pakistan

Special Acknowledgement:

Mr. Muhammad Farooq, Director, PTA & Head of COP Committee, Mr. Ahmed Bakhat, Director, PTA & Member of Committee, Samreen, Deputy Director & Member of Committee, Ms. Zaib Unisa Gharshin, Deputy Director, PTA & Member of Committee, Mr. Adil Javed, AD Law, PTA & Member of Committee, Waqas Hassan, AD, PTA & Member of Committee, Mr. Hamza Ahmad Sial, AD, PTA & Member of Committee, Mr. Waleed Ahmed, AD, PTA & Member of Committee

Book Designed by: Faiq Ahmed & Sualeha Ahmed Jalbani
Illustrated by: Shafaq Bashir Muhammadi, Sualeha Jalbani
Content Direction: Faiq Ahmed, Aatika Saleem, Maliha Jalal
Support Design: Hafsa Bano, Hania Zubair,
Umair Najeeb Khan, Mahnoor Salman, Rameen Pai

Special Thanks to

Zara Basharat Higgs - Head Public Policy Programs South Asia, TikTok
Fahad Khan Niazi - Head of Government Relations & Public Policy
Emerging Markets, TikTok
Dr. Aamna Pasha - Chief Academic Officer, Zindagi Trust
Tazeen Hussain - Head of Communication Design Department, IVS

We would like to express our gratitude to
Indus Valley School of Arts and Architecture and Telecom Foundation
for their invaluable support throughout this project.

TABLE OF CONTENTS

1

Introduction

2

Social Media and
Digital Safety

4

Safeguarding our
Digital Self on
Social Media Apps

3

Dangers of the
World of Social Media



5

Safe Tiktoking

6

**Becoming a Responsible
Digital Citizen**

7

**Cyber Law in
Pakistan**

8

Quick Review



Let's learn together!

A component of our lives now exists digitally in the form of our social media accounts, which we use to share aspects of our lives.

From the comfort of our room, we connect with the whole world.





36%

of the people
in Pakistan have
access to the internet

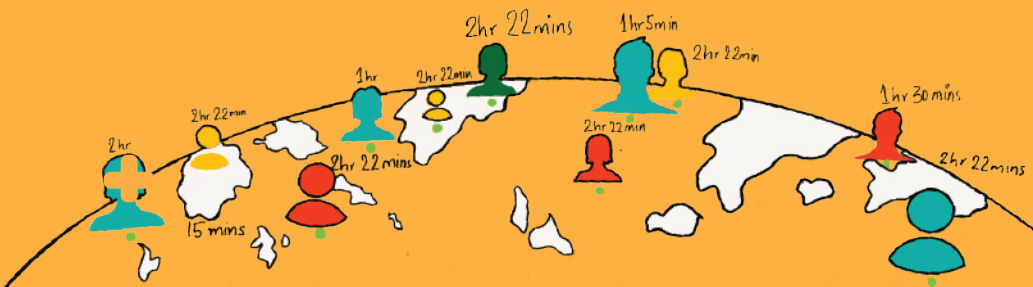
51%

of the world's population
or over is online right now!

2 Hours and 22 Minutes

are spent by internet users on
social media on an average in Pakistan

Source: Datareportal - Global Digital Insights (Digital 2023: Pakistan)



Social Media and Digital Safety

Digital Safety means protecting yourself and your:



Mobile Devices



Social Media Accounts



Personal Profiles



Computers/Laptops



Personal Information

The internet connects us globally, allowing us to **find information, learn, stay updated & share entertaining content with friends and family.**

While the internet may be fun and entertaining, it can also harm us in various ways such as **hate speech, bullying and misinformation.**

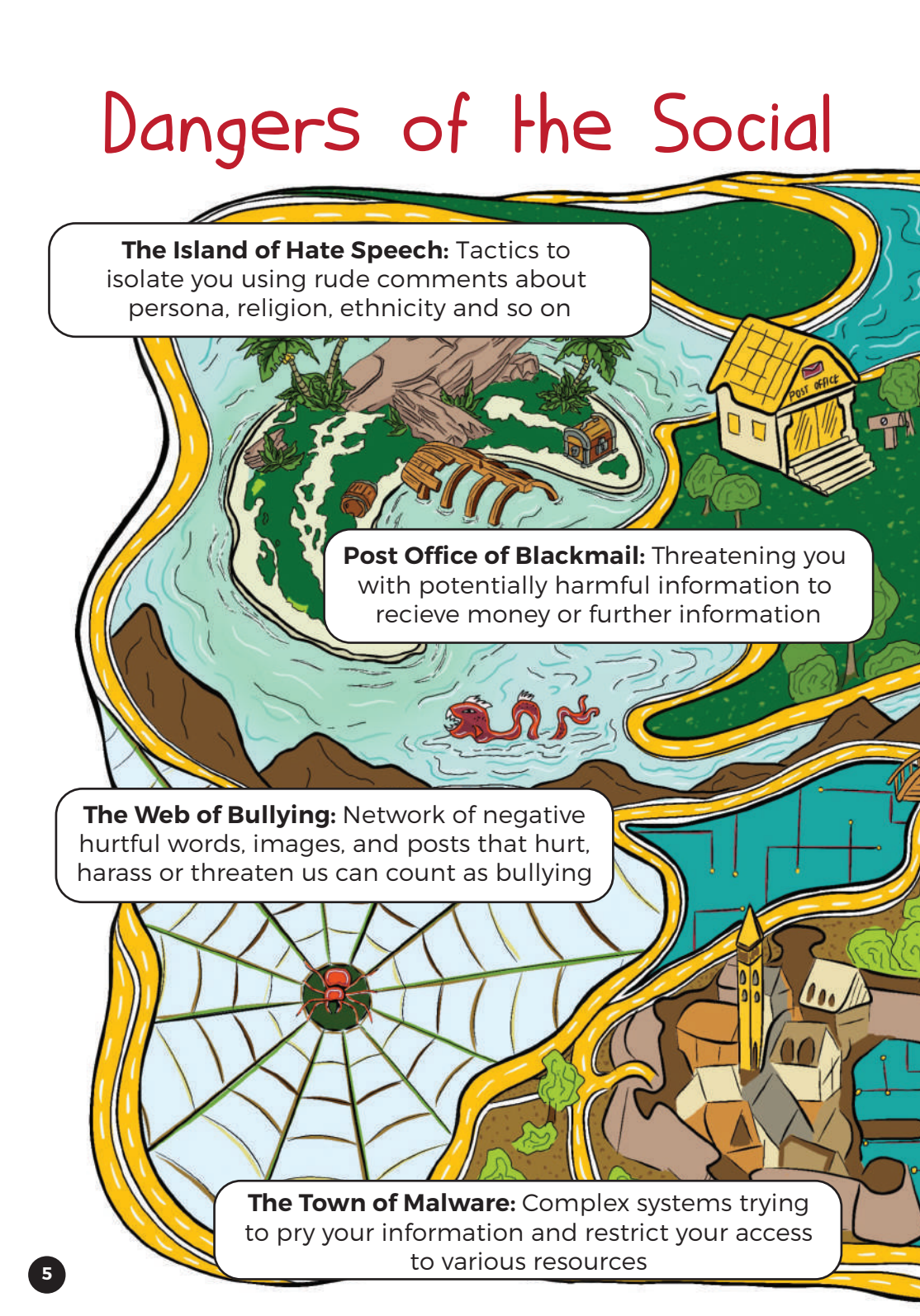
But fear not!

Fortunately, these social media platforms provide us with tools to **protect ourselves and safeguard our safety and privacy.**

We just need to be mindful of our safety in any online space.



Dangers of the Social



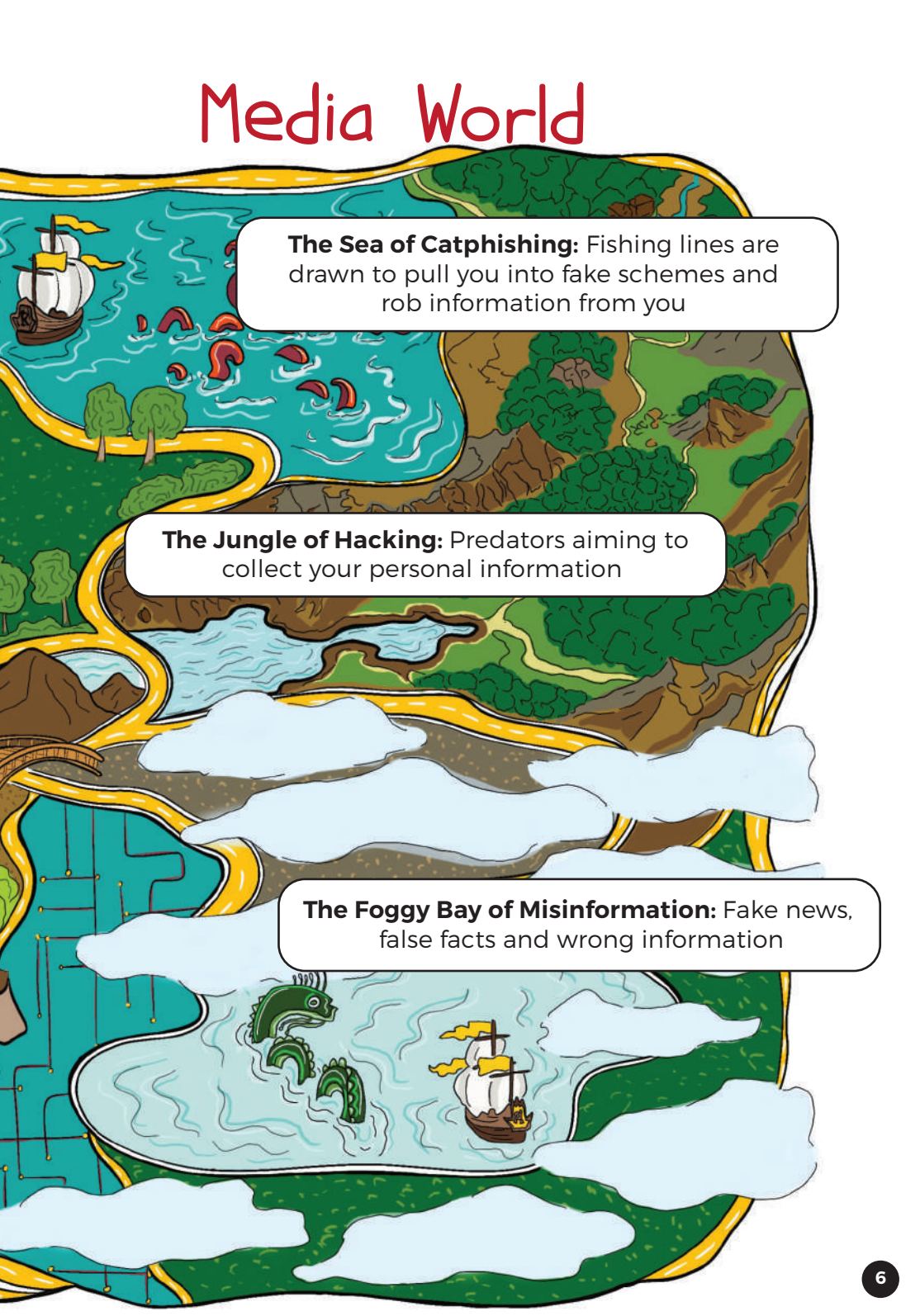
The Island of Hate Speech: Tactics to isolate you using rude comments about persona, religion, ethnicity and so on

Post Office of Blackmail: Threatening you with potentially harmful information to receive money or further information

The Web of Bullying: Network of negative hurtful words, images, and posts that hurt, harass or threaten us can count as bullying

The Town of Malware: Complex systems trying to pry your information and restrict your access to various resources

Media World



The Sea of Catphishing: Fishing lines are drawn to pull you into fake schemes and rob information from you

The Jungle of Hacking: Predators aiming to collect your personal information

The Foggy Bay of Misinformation: Fake news, false facts and wrong information

Word Search

Look for the words listed below



Answer Key:

Misinformation, Cyberbullying, Hate Speech,
Malware, Hacking, Catfishing, Blackmail



Misinformation

Misinformation is false or misleading information that can be harmful as it leads us to believe things that are not true.

It is essential to be cautious about the online content we consume.

Rumors, in particular, are unattributed and unreliable information that is often unverified. They can either be:

TRUE

FALSE

We must take care to ensure that the information we share with others is true and based on verified facts.

Verify the information by looking for authentic sources such as:



Academic & Research Papers



Official Government Websites



News Channels or Websites



Fact-Checking Websites



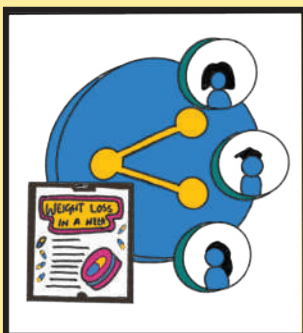
Misinformation
is Misleading!

Consequences of Misinformation

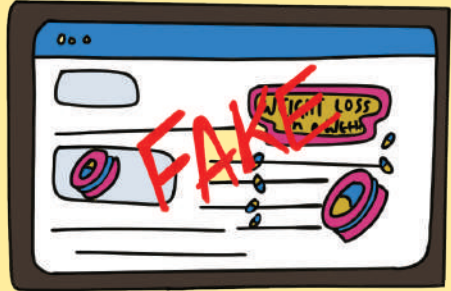
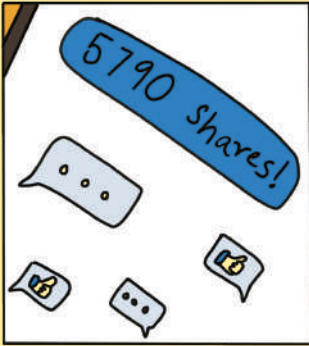


Fatima loves spending time on social media. She likes to read the latest news and share interesting articles with her friends

One day, she came across an article that claimed a certain medicine can make you lose weight in a week



Many people had already shared the article, and it had gone viral, causing **confusion and misinformation**



She did some research and found out that the claim was **false and harmful**

From that day onwards, Fatima became more aware of the potential of misinformation online and made sure to always check the sources and facts before sharing any news and articles online



Protection Against Misinformation

We need to stay vigilant to get correct information on the internet

Ensure the source is reliable before trusting the information

Do not believe information from Social Media Groups, even if it comes from trusted adults. It could be false

Verify any information with a credible source before sharing it forward



Activity

Verify if the following statements are true.

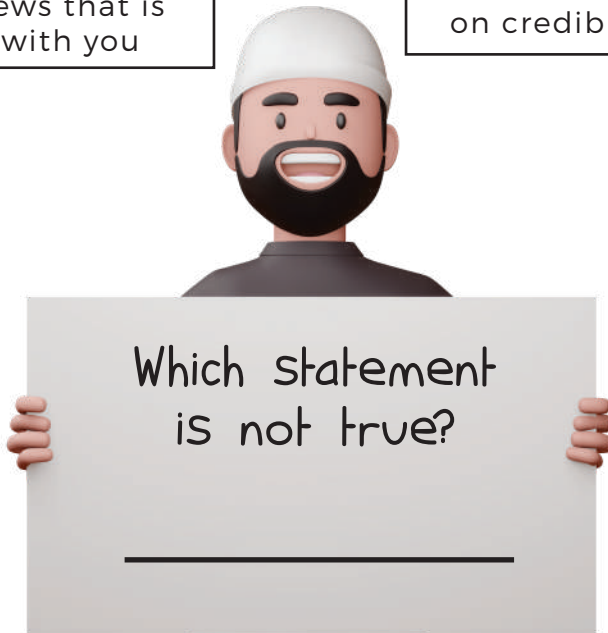
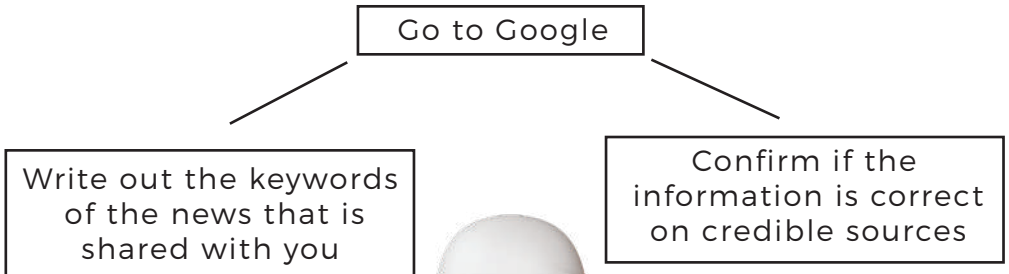
Statement A 

Karachi will receive snow next year, report says.

Statement B 

In a recent cricket match, Babar Azam took 5 wickets.

How to verify misinformation



Cyberbullying

Cyberbullying is online bullying that involves using digital platforms to intimidate, harass, or demean others.

It includes actions like sharing:



Harmful
Content



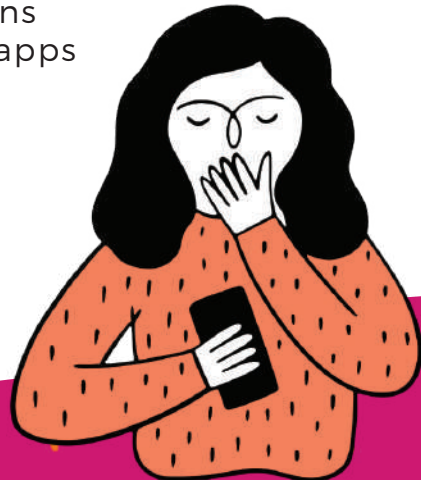
Personal
Information



Causing
Embarrassment

To prevent Cyberbullying:

- Promote a safe online environment
- Identify unknown sources
- Protect mobile devices
- Use secure internet sources
- Stay vigilant
- Be mindful in online interactions
- Implement privacy settings in apps
- Encourage reporting
- Report inappropriate content/comments



Hate Speech

Hate speech involves offensive language targeting individuals or groups based on characteristics like race, religion, or gender, posing a threat to social peace.

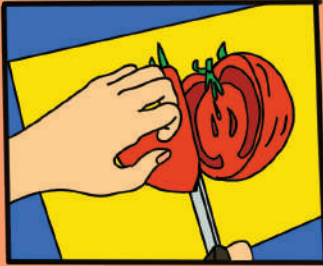
It is important to recognize the detrimental effects of hate speech as it can lead to mental strain and discomfort.

Maintain a safe online circle and avoid dangers like hate speech and cyberbullying and surround yourself with individuals who promote positivity and respect.

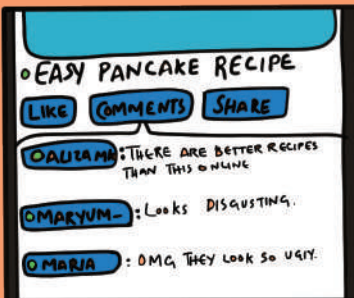
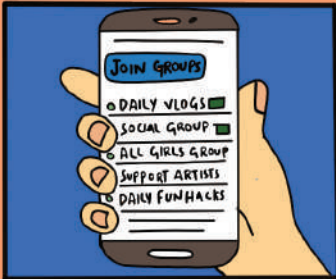


**AVOID OFFENSIVE
COMMENTS!**

Confronting Cyberbullying and Hate Speech



Fatima loves to cook & try out new recipes, she also loves making cooking videos and sharing them with friends



At first, it was just a few mean comments on her post but soon the messages became more personal & vicious



Fatima tried to ignore them, but the messages kept coming and the situation got worse

Fatima became isolated and heartbroken. She felt like she had nowhere to turn



When she confided in her teacher, she realised, she does not have to face this alone



The teacher helped her report the malicious comments. Fatima's social media was now dominated by her safe friend circle and became the center of positivity

Protection Against Cyberbullying and Hate Speech



Do not be afraid to take action against
Hate Speech or Cyberbullying

To protect yourself against **cyberbullying & hate speech**:

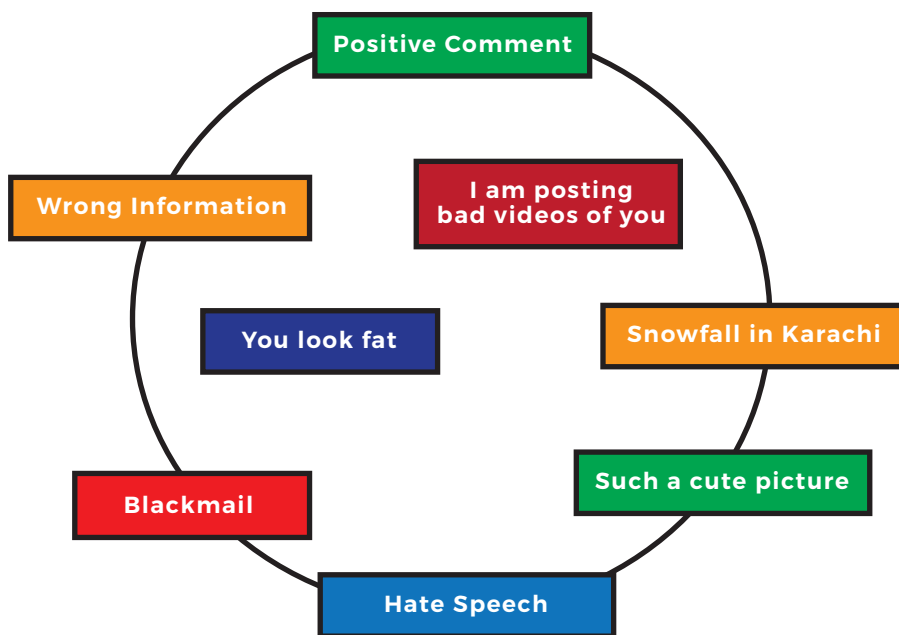
- Set **video keyword filters**
To learn how, move to page 43
- Block individuals from accessing personal information and accounts
- Seek guidance from a trusted adult for troubling online content

Keep in mind, seeking support from trusted adults demonstrates strength and maturity

Stay safe by standing up to Cyberbullying and Hate Speech

Connect the dots with matching keywords to create a constructive online environment.

Avoid overlapping lines.



What safety measures do you use right now to ensure a healthy, positive experience on social media?

Strong Passwords

2 Factor Authentication

Avoid Oversharing

Privacy Settings

Report and Block

Malware

Malware is a file that hackers use to infect, steal, or control devices. It can spread through:



Email Attachments



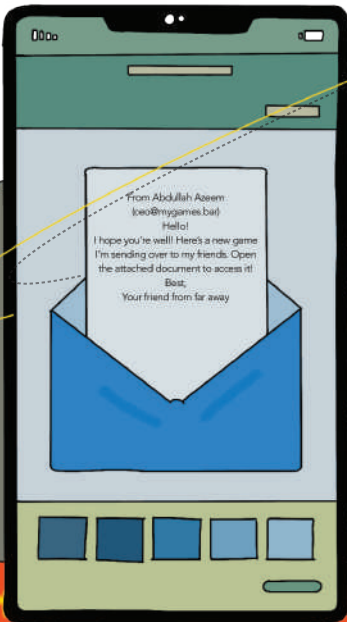
Deceptive Websites



Fake Social Media Ads

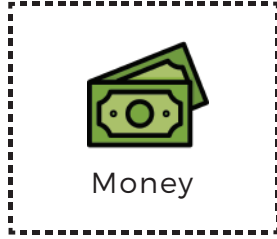
Malware operates secretly, leading to data loss and potential exposure of **personal, financial, and contact details**.

Notice how it does not look dangerous at all but may potentially gain access to your mobile phone and steal your personal information!



Hacking

Hacking refers to unauthorized access to your social media accounts, often achieved through password guessing or deception. It can result in loss of:



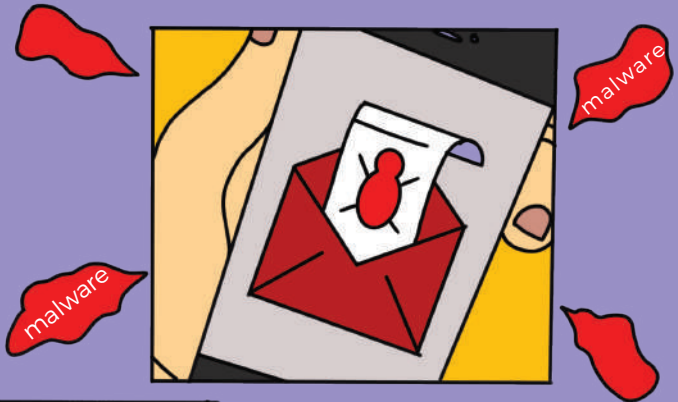
Hacking is a cybercrime with serious implications.



**BE AWARE
OF HACKERS!**

Malware and Hacking: A Cautionary Tale



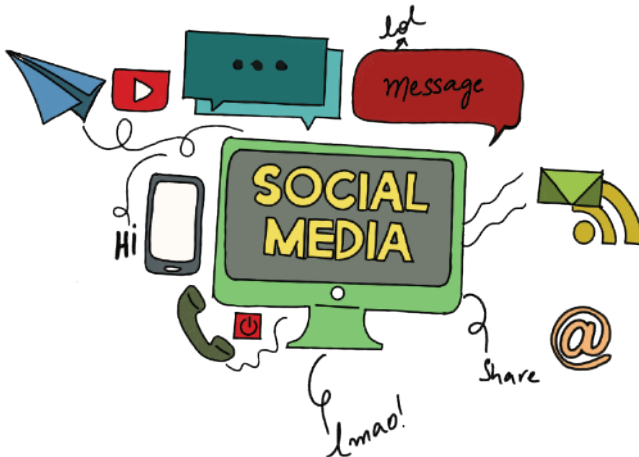


From that day forward, Fatima became more careful about clicking on links from unknown sources

She learnt the importance of staying vigilant and protecting herself from **cyber threats**. She also made sure to install an antivirus app on her phone to keep it safe from future attacks

Protection Against Malware and Hacking

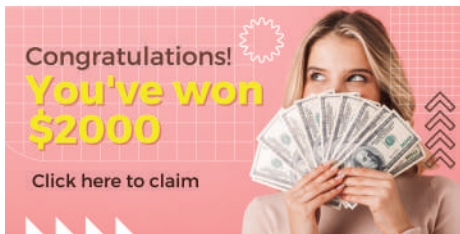
- **Verify the sender's email**, check hyperlinks, website URL and use anti-phishing software and browser extensions for protection
- **Use strong passwords.** Set a combination of uppercase and lowercase letters, numbers, and symbols, and avoid using easily predictable information like birth dates or common words
- **For example:** rather than setting your password to purple1591! you should rephrase it to P0rpL31591!
- **Limit mobile application permissions** when you are asked to give access to your devices
- **Avoid unknown USB drives.** Scan any USB device before accessing it on your computer
- **If the dialogue box of the installation software does not match the original logo and text description of the software you want to download; it is best to check its validity.** If it does not seem legitimate stop the installation process or uninstall the software



The goal of this activity is to color the **Digital Safety Tower** completely. Each right answer gets you **50 points** while a wrong answer deducts **50 points**.

Choose the correct option carefully keeping in mind the content you have read above.

Question 1:
Which Advertisement is safe to click?



(Option A)



(Option B)

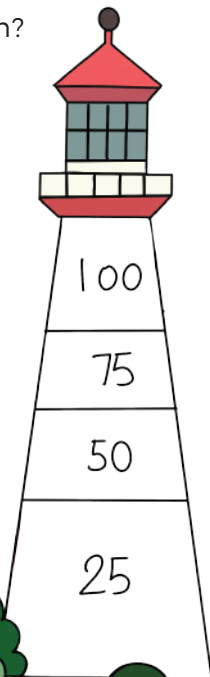
Question 2:

How would you react to the following situation?

Your social media account has expired, please provide the following information to restore your account.

- Father & Mother Name
- Full Name
- Date of Birth

- A) Ignore
- B) Report
- C) Reply



Catphishing, Phishing, Clickbait and Scams



Catphishing is when someone creates a false identity using others' information and images.



Phishing is a fraudulent attack that aims to steal personal information by tricking victims into disclosing it on fake websites.



Scams aim to steal money and personal information by tricking victims into revealing sensitive details like credit card numbers and passwords on deceptive websites.



Clickbait uses misleading headlines to attract clicks on content by exaggerating or omitting key details.



Blackmailing

Online blackmailing involves threatening to expose personal information or media to the public, friends, or family unless demands are met. It may include sensitive content, images, videos, or voice notes



Do not engage with blackmailer and take the matter to a trusted adult immediately!

A trusted adult plays a vital role in providing support, guidance, and protection.

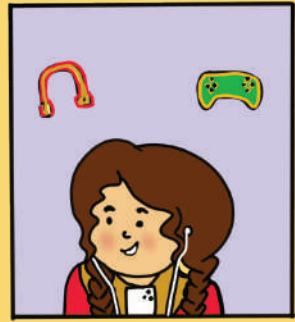
They can offer empathy, assist in reporting the incident, provide necessary advice, and potentially mediate or intervene.

Their role extends to educating and empowering you to prevent such incidents in the future.



**This is
an Attack**

Fatima's story about Blackmailing and Scam

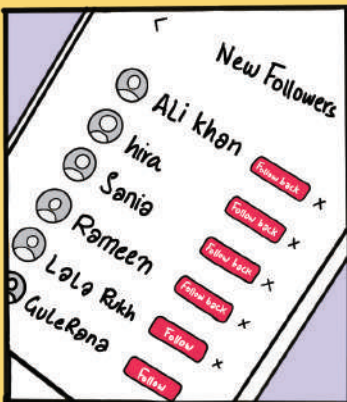


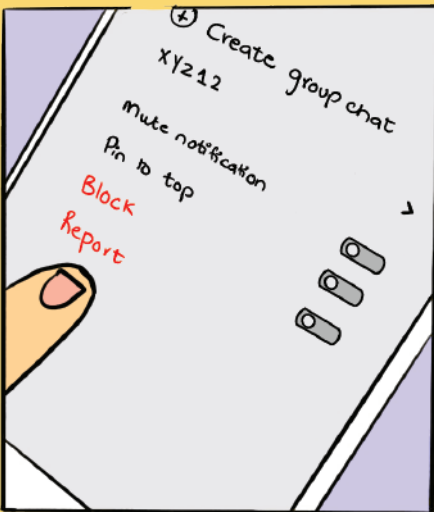
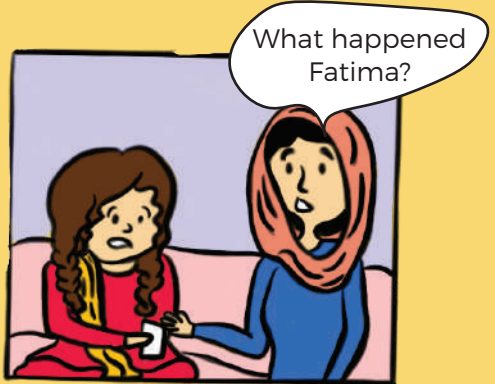
Fatima loves spending time online

She likes to chat with her friends, play games & share pictures on social media

One day, she received a friend request from someone with the same name as her friend and they started chatting

Fatima was getting closer to her friend. However, with time the messages got scarier asking her for inappropriate information and pictures





Her mother instructed Fatima to **block and report** the account. From that day, Fatima only added and communicated with people she knew and trusted.

Protection Against Blackmailing and Catphishing



- Be cautious about sharing personal information online such as full name, address, phone number, or school name with strangers
- Set strict privacy settings on social media profiles and limit the visibility of personal information to only friends and family
- Avoid engaging with strangers or suspicious individuals online, including accepting friend requests or clicking on links from unknown sources
- Report any suspicious or abusive behaviour online to a parent, teacher, and trusted adult
- Exercise caution when encountering emails, messages, or phone calls that request personal information, as they may be fraudulent or malicious in nature

If you ever face this situation
what would be your response?



Hello! I'm calling from Pakistan's most successful gaming company today. I am very excited to announce that you have won a prize worth Rs. 100,000 on completing Level 25 of the game!

We have seen your skills and would like to offer you this money.

Umm okay, what details do you want?



We just need your personal information and we will then deposit the winning cash prize in your bank account. Please tell us your card and banking details?

Write your response here:



Guidelines for sharing Visual Media



Be extra vigilant, especially about the nature of images, and videos you are sharing online. Once you post something you can no longer control who uses your images, for what purpose.



Be cautious about what you share and with whom. Strange people may access your images and use them to exploit you.



Respect yours and other's privacy online. Sharing explicit images or videos of yourselves or others, even among friends, can have serious consequences. Understand that what you share online can stay online forever. Content "leaked" or shared non-consensually can be distressing.



Learn how to recognize inappropriate content while browsing the internet. This can be any image or video that makes you uncomfortable or confused.



If you do come across such content, tell a trusted adult right away. Immediately exit the page, talk to a trusted adult, and report the content to the appropriate authorities.



Knowing consent and boundaries is cool! Understand that sharing explicit content without consent is not only illegal but also disrespectful and harmful.

What is "Consent?"

Take consent even for simple things like taking a picture, borrowing something etc.

Ensure that your friends or anyone say 'yes' before you proceed. If they say 'no' for any reason, respect their choice

Given consent can be taken back. People change their minds. It is completely fine

Remember to use kind words when asking for consent



Snakes and Ladder Cyber Edition

30 **Sharing personal information with strangers online**

29 **Sharing personal information with strangers online**

28 **MAMA MAMA**

27 I will keep my information and passwords a secret

26 I will keep my information and passwords a secret

25 **Sharing your pictures publicly**

24 **MAMA MAMA**

23 I will not be unkind to anyone online

22

21

20 If someone online asks me to meet them I will always talk to an adult first

19 I know that on the internet, people are strangers and they may not be who they say they are

18

17

16 **MAMA MAMA**

15

14 I know online content have copyrights

13

12

11

10 **Sharing and forwarding unverified information**

9

8 I only open messages that are safe, if I'm unsure I will ask an adult first

7

6 I always check if the information online is true

5

4

3 Adults know which websites and apps I use or surf

2

1 **Online**

WINNER
You are a Digital Safety Champion

COLOUR ME



Safeguarding our Digital selves

We need to understand that protection is better than the potential consequences of upsetting online incidents. We can stay safe, and it is really easy!

Learning about privacy settings and other safety features on social media apps will help us enhance our online experience and make it safer.

It is our responsibility to effectively use these safety tools and settings to safeguard ourselves.



Two-Factor Authentication

Two-Factor Authentication (2FA) is an added security layer for social media platforms. Users provide two forms of identification for account access.

The common method is receiving an SMS code on a mobile phone, but alternatives exist.

Those without personal phones can use a trusted family member's phone or opt for email-based confirmation.

A trusted family member's phone can be used in either case. Authentication apps generate secure codes on accessible devices.

Enabling Two-Factor Authentication enhances account security.



Unfollow, Mute, Unfriend and block



You can unfollow or unfriend someone bullying you or demanding unethical/unlawful information or content

Use **Mute** to stop seeing posts from someone without unfollowing them

Block and report someone if they are sending you harmful, unwanted messages or comments

Filtering Comments



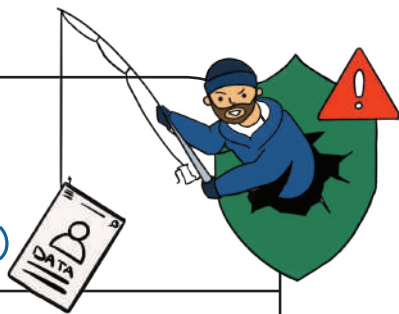
Turn on the comment filters to block out any inappropriate or offensive comments

Report any comments that are harmful or harassing

Delete any comments that makes you feel uncomfortable or upset

Content Privacy

(Private, Friends, Family, Close Friends and Public)

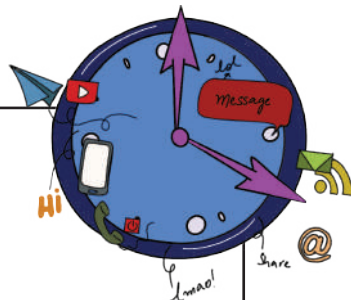


Control privacy settings to manage post and profile visibility

Keep personal information such as address, phone number, and email address private

Be cautious when sharing photos and videos online and consider your audience

Tracking your time on Social Media Platforms

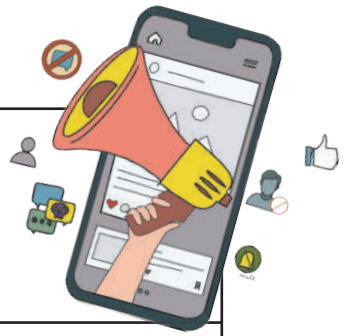


Utilize social media app's tracking and time limit setting tools, these tools can be found in account settings

Take breaks from social media to avoid feeling overwhelmed or becoming addicted

Be mindful of the impact of social media usage on daily activities

Managing Unwanted Direct Messages



Ignore any messages from people you don't know or trust

If someone is sending you unwanted messages, **block them!**

Report any inappropriate or harassing messages to the social media platform

Reporting unwanted, Explicit Content



Report any explicit or inappropriate content to the social media platform

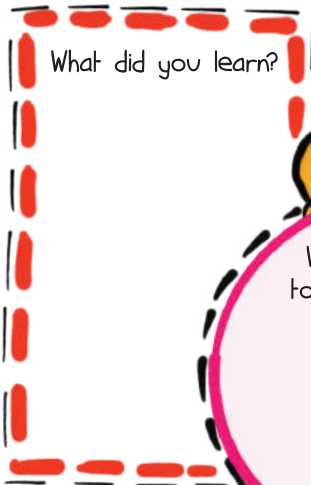
On Tiktok, this can be found in the share icon (➦) option

Be aware of what inappropriate content is

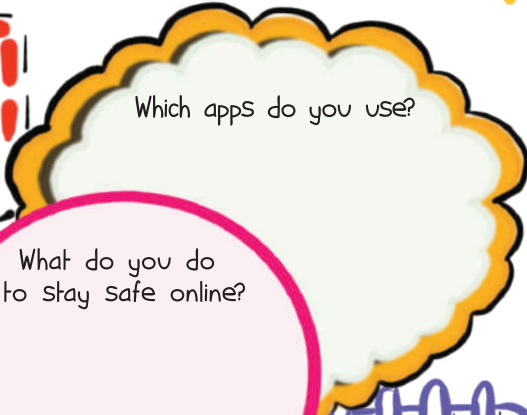
Don't share or forward explicit content

Journaling

Your Name:



What did you learn?



Which apps do you use?



What do you do to stay safe online?



Your thoughts?



What do you not like about social media apps?

One Month Challenge

Week 1

My weekly app activity tracker			
Name of the Social Media App			
Monday			
Tuesday			
Wednesday			
Thursday			
Friday			
Saturday			
Sunday			

Week 2

My weekly app activity tracker			
Name of the Social Media App			
Monday			
Tuesday			
Wednesday			
Thursday			
Friday			
Saturday			
Sunday			



Week 3

My weekly app activity tracker			
Name of the Social Media App			
Monday			
Tuesday			
Wednesday			
Thursday			
Friday			
Saturday			
Sunday			

Week 4

My weekly app activity tracker			
Name of the Social Media App			
Monday			
Tuesday			
Wednesday			
Thursday			
Friday			
Saturday			
Sunday			






Safe TikToking:

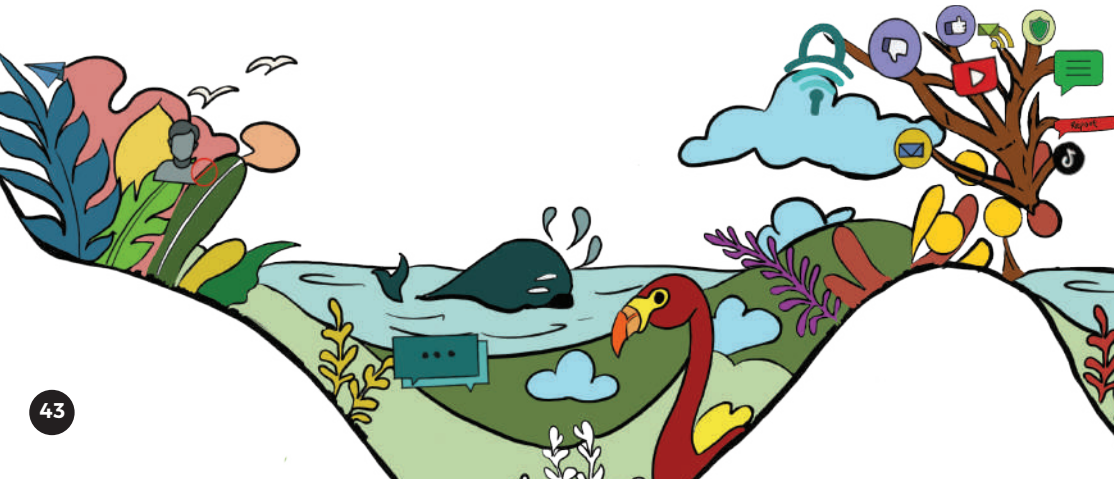
TikTok provides a number of safety tools and resources that allow you to control your privacy preferences and access most relevant and appropriate content.

Restricted Mode:

Restricted mode on TikTok limits exposure to content that may not be suitable for everyone. If you find a video on your feed that you think should be restricted, you can report it or you can turn on Restricted Mode through the following settings:

How to turn on Restricted mode:

- In the TikTok app, tap **Profile**  at the bottom
- Tap the **Menu**  button at the top
- Tap **Settings and Privacy** 
- Tap **Content preferences** 
- Tap **Restricted mode**
- Turn **Restricted mode** on 
- Follow the instructions to **set a passcode** for **Restricted mode**



Video Keyword Filters:

This feature enables you to customize the content within your "**For You**" and "**Following**" feeds.

To add video keyword filters :

- In the TikTok app, tap **Profile** 👤 at the bottom
- Tap the **Menu** ☰ button at the top
- Tap **Settings and Privacy** ⚙️
- Tap **Content preferences** 🗑️
- Tap **Filter video keywords**
- Tap **Add keywords** Add keyword
- Enter **a word** or **a hashtag** you would like to filter
- Select the feeds you'd like to filter it from (**For you or Following**)
- Tap **Save** to confirm

Mark videos as 'Not Interested':

- In the TikTok app, press and hold on the video, or tap the **Share** ➦ button on the side
- Tap **Not interested** 🖤
- You will not see content similar to the marked video

To delete or edit filtered keywords:

- In the TikTok app, tap **Profile** 👤 at the bottom
- Tap the **Menu** ☰ button at the top
- Tap **Settings and Privacy** ⚙️
- Tap **Content preferences** 🗑️
- Tap the **Delete** 🗑️ button next to any keywords you would like to remove
- Tap **Delete** to confirm



Reporting a video:

If you find a video that is inappropriate or improper you can report it by doing the following:

- In the video playing page, select the **Share** ↗ button
- Tap the **Report** 🚩 button
- Select a reason accordingly
- Tap **Submit**

Reporting a Comment:

- **Long press** the comment you would like to **Report**
- Tap **Report**
- Select a reason accordingly
- Tap **Submit**

Blocking an account:

- Open the profile you would like to **Block**
- Tap **Share** ↗ at the top right corner of the app
- Select **Block** 🚫 accordingly
- Tap **Block**

Reporting an account/content:

- Open the profile you would like to **Report**
- Tap **Share** ↗ at the top right corner of the app
- Select **Report** 🚩 accordingly
- Select your preferred option



Trusting your Parents - a two way street

Openly sharing online risks and concerns with parents or a reliable adult can be really helpful in addressing any challenges in your life.



1

Avoid waiting to be in a risky situation to talk to someone



2

Ensure online safety by promptly notifying adults about any online activities, allowing them to intervene against potential harm or discomfort



3

Build relationships with parents and adults through patience and open communication



4

Keep in mind the generational gap when discussing the online world with parents

Becoming a Responsible Digital Citizen

Making the internet a safe space for other digital citizens and yourself is a process that goes hand in hand. Remember to treat others the way you want to be treated and create an environment you would like to be online in.

Here are some guidelines to follow:

- Be respectful and expect respect from others as well
- Show empathy online
- Avoid judging others
- Think before you make a comment
- Protect your privacy
- Be mindful of your tone
- Verify any information/news before sharing it
- Report any harmful content you come across
- And most importantly, be kind



Know it all!

For this activity, sit with your trusted adult and get ready to know them more! Your trusted adult will write answers for you while you will write answers for your trusted adults.

For example, if the question is,
“What is your favourite picnic spot?”

You will write what you think is your guardian’s favourite picnic spot and they will write what they think is yours!

Wait till you both have written your answers.

Reveal the answers. See who has answered the questions correctly!

The person who gets the answers wrong may do dares at the end of each question.

“Feel free to make your own silly dares!”

What is their
Favourite App?

What is their
Favourite App?

What do you
like about
social media?

What do you
like about
social media?

What do you
dislike about
social media?

What do you
dislike about
social media?



ZINDAGI
TRUST



DIGITAL حفاظت

Guidelines for Children



Cyber law of Pakistan

Our government helps us in staying safe and legally protected online. Pakistan has laws in place to protect the digital rights of its citizens

- **Cyber Crime Wing (CCW), FIA** can facilitate you in registering your complaint
- Remember to report cybercrime responsibly and avoid making false or vindictive reports

Official Contacts for Reporting

- Use the **Cyber Crime Wing (CCW), FIA official website** to report phishing and other online crimes

FIA Cyber Rescue Helpline number: 9911

Website: www.complaint.fia.gov.pk

Email address: complaints@fia.gov.pk

- Use **Pakistan Telecommunication Authority (PTA)**, the regulatory body for Telecom services in Pakistan, to report unlawful content blocking/removal

Helpline number: 0800 55055

Website: www.pta.gov.pk



Gender Protection Unit

The Gender Protection Unit serves as a safeguard for women and children, providing a platform to address incidents of harassment and blackmail.

Individuals can rely on this unit to lodge complaints and seek appropriate action against such incidents

www.complaints.islamabadpolice.gov.pk

Digital Rights Foundation

Digital Rights Foundation can be reached out to for Cyber Harassment. You can contact them at:

Helpline Number: 0800-39393
helpdesk@digitalrightsfoundation.pk

This helpline is operated **7 days a week**
from **9 am - 5 pm**

Rozan

Rozan is an organization that collectively works with individuals, vulnerable groups and institutions on promoting emotional health, tolerance, gender equality and reducing violence against women and children.

They have variety of programs for children, women, men and police personnel.

Rozan counseling helpline: 0304-111-1741

Quick Review



Ensure Digital Safety by protecting yourself and your online presence from potential harm

Maintain open communication with a trusted adult



Be aware of and learn to protect yourself from social media dangers like malware, blackmail, hacking, phishing, bullying, and hate speech

Use safety controls on TikTok and other social media apps for your protection



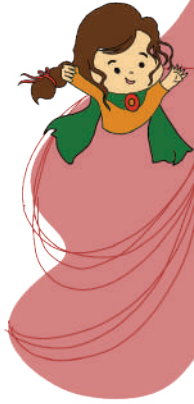
Be a mindful responsible digital citizen when online



Stay informed about the various official contacts as they are crucial for online safety



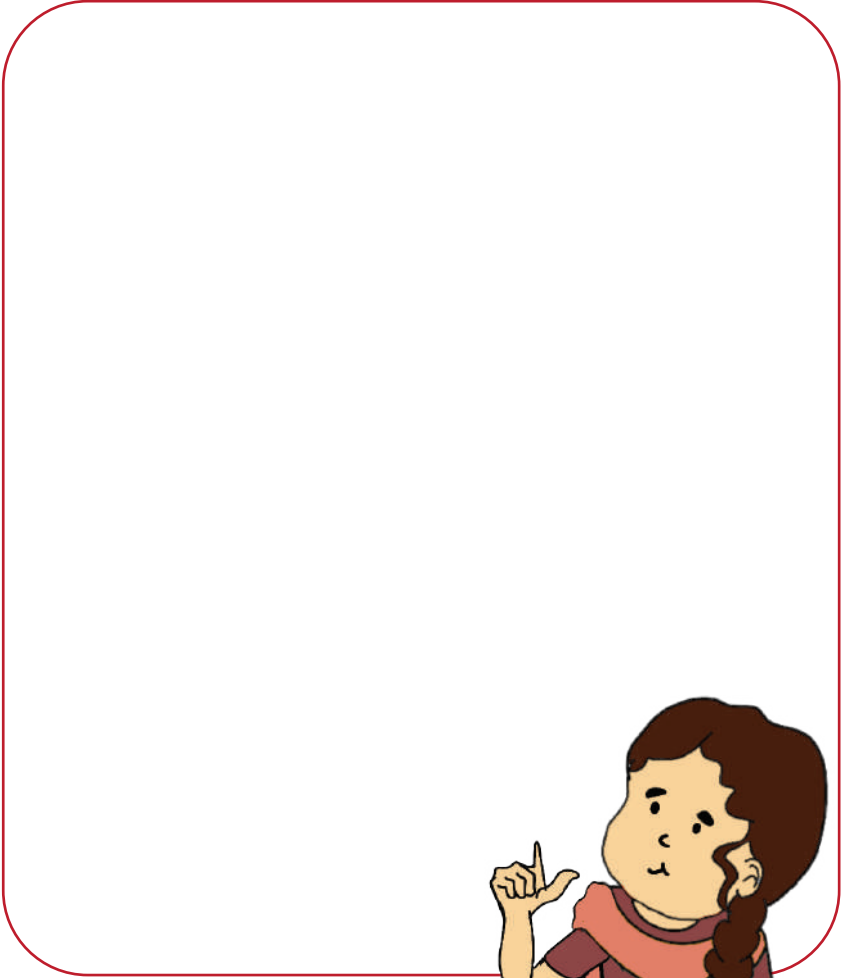
Make your own
Digital super hero



Help the children get to the middle of the maze and color the safety zone



What did you learn?



DIGITAL حفاظت



ZINDAGI
TRUST



A project ensuring Digital Safety across Pakistan
for children, parents and teachers.

