



Gurukul Technicals Institute

Computer education · Robotics · Science projects · Delhi

FREE EBOOK

ENGLISH, CAREERS AND VOCATIONAL SKILLS

Cyber Safety for Students and Parents

Stay safe on phones, social media and games

INSIDE THIS BOOK

- Your digital footprint
- Strong passwords and two-step verification
- Privacy settings
- Sharing photos safely
- ...and 7 more chapters, practice questions and a glossary

Beginner

Students of class 5 to 12 and their parents

engineergurukul.com

+91 97116 99511

Cyber Safety for Students and Parents

A friendly guide for students of class 5 to 12 and their parents. Learn how to protect your accounts, set up privacy, share photos wisely, deal with bullying, spot grooming, fake news and scams, balance screen time with sleep, and report problems through 1930 and cybercrime.gov.in. It ends with a family agreement you can fill in together.

WHO IT IS FOR	Students of class 5 to 12 and their parents
LEVEL	Beginner
SUBJECT AREA	English, careers and vocational skills
WHAT IS INSIDE	11 chapters, practice questions with answers, and a glossary

HOW TO USE IT

Read one chapter at a time and try the examples as you go: on a computer, at your workbench or in your notebook. The boxes give tips, safety points and short activities. When you finish, test yourself with the practice questions and check your answers at the end. Words you may not know are explained in the glossary.



Gurukul Technicals Institute

A-10, Chief Commissioner Colony, opposite Rana Pratap Bagh, Delhi 110007
Phone 011 2721 1512 · Mobile and WhatsApp +91 97116 99511
engineergurukul@yahoo.co.in · engineergurukul.com

Free ebook. You may read, print and share this ebook for learning. It may not be sold or changed.

© 2026 Gurukul Technicals Institute. First edition, October 2026. The information was checked when it was written; software, prices and rules change, so for anything official always check the latest source.

What you will find inside

1	Your digital footprint	5
2	Strong passwords and two-step verification	6
3	Privacy settings	8
4	Sharing photos safely	10
5	Cyberbullying and what to do	12
6	Online friends and grooming warning signs	13
7	Fake news and checking facts	15
8	Gaming safety and in-app purchases	17
9	Phishing and scams	18
10	Screen time and sleep	20
11	Reporting and your family agreement	22
	Practice questions	24
	Answers	26
	Glossary	27

Your digital footprint

Every time you use the internet, you leave marks behind, like footprints on a wet floor. Your digital footprint is the trail of everything you do online: the photos you post, the comments you write, the videos you like, the games you play and the things you search for. It also includes what other people post about you.

Two kinds of footprint

- **Your active footprint** is what you share on purpose: a post, a comment, a photo in a group chat.
- **Your passive footprint** is what is collected without you noticing: the websites you visit, your location, and what apps record about how you use them.

Why it matters

The internet has a long memory. Even if you delete a post, someone may already have taken a screenshot (a picture of the screen) or forwarded it. A rude comment you write at 13 could be found when you apply to a college or for a job years later. On the good side, a careful footprint can show your talents: a science project video, a drawing, or a kind message to a friend.

EXAMPLE

Rhea, in class 9, posted a joke about her maths teacher in a class group. She deleted it after ten minutes. By then, three classmates had taken screenshots, and one of them reached the teacher. Rhea learned that "delete" does not mean "gone".

The hoarding test

Before you post anything, imagine it printed on a giant hoarding at the busiest crossing in your town, with your name and photo beside it. Would you be happy for your parents, your teachers and your neighbours to see it? If not, do not post it.

TRY THIS

Search for your full name online, with and without your city. Look at what comes up. If you find an old account you no longer use, log in and delete it, or ask a parent to help you.

NOTE

For parents: your posts are part of your child's footprint too. A photo of your child in school uniform, with the school name showing, tells strangers where to find them. Ask older children before you post pictures of them, and set your own accounts to private.

CHAPTER 2

Strong passwords and two-step verification

Your password is the key to your online life. If someone gets it, they can read your messages, pretend to be you, and even lock you out of your own account.

Weak and strong passwords

Weak password	Why it is weak
123456 or password	One of the first things attackers try
priya2012	Your name and birth year are easy to guess
9876543210	Your phone number is known to many people
The same password everywhere	One leak opens every account

A strong password is **long, hard to guess** and **used only once**. The easiest way to make one is a passphrase: three or four random words joined together, with a number or symbol added. Aim for at least 12 characters. A passphrase built from words that have nothing to do with you is easy to remember and very hard to guess. Make up your own; never use an example from a book.

Five password rules

1. Use a different password for every important account, especially email, social media and games.
2. Protect your email password most of all. If someone controls your email, they can reset the passwords of all your other accounts.
3. Never share your password with friends, even your best friend. Friendships change, and a shared password can be misused after a quarrel.
4. Do not save passwords on a shared or public computer, such as one at a cyber café.
5. If you think a password has leaked, change it at once.

REMEMBER

An OTP (one-time password) is a short code sent to your phone. Never tell anyone an OTP sent for a login, a payment or an account change. A bank, a game company or a police officer will never ask you for one. Anyone who asks for such an OTP is trying to get into your account.

Two-step verification

Two-step verification (also called two-factor authentication) means you need two things to log in: your password, and a second proof that it is really you. The second proof may be a code sent by SMS, a code from an authenticator app, or a tap to approve a prompt on your phone. Even if someone steals your password, they cannot log in without the second step.

Turn it on for your email, social media and gaming accounts. You will usually find it in the account's security settings.

If your account is hacked

1. Use the app's "forgot password" or account recovery option at once, and set a new, strong password.
2. Change the password of your email, and of any account that used the same password.
3. Turn on two-step verification.
4. Tell your friends not to trust strange messages from your account, because hackers often use a stolen account to trick friends.
5. Report the problem to the app, and tell a parent.

TIP

Lock your phone with a PIN, pattern, fingerprint or face unlock, and never leave it unlocked on a desk. Install updates for your phone and apps when they arrive, because many updates fix security weaknesses.

CHAPTER 3

Privacy settings

Privacy settings decide who can see your posts, who can contact you and what an app knows about you. When you first install most apps, these settings are often more open than you would like. Spend ten minutes setting them up properly.

Settings to check on every app

1. **Make your account private**, so only people you approve can see your posts.
2. **Check your followers or friends list**. Remove anyone you do not know in real life.
3. **Limit who can message you**, tag you in posts and comment on what you share.
4. **Hide your phone number and email address** from your profile.

5. Turn off location on posts, and share live location only with family.

What to keep off your profile

Your profile should not show your full date of birth, your school's name, your home address, your phone number or your daily routine. A stranger who knows your school and your tuition timings knows where you will be, and when.

EXAMPLE

Sana, in class 10, checked her followers list one Sunday. She had 312 followers but knew only about 140 of them in real life. She removed the rest, made her account private, and hid her phone number. It took her twenty minutes.

App permissions

A permission is something an app asks to use: your camera, microphone, contacts, photos or location. A torch app has no reason to read your contacts. In your phone's settings, look at the list of apps and the permissions each one has, and switch off any that are not needed.

DID YOU KNOW

Most social media apps say in their rules that users must be at least 13 years old. These rules exist because younger children are at greater risk online. Starting at the right age, with a parent's help, is the safest way.

Check again every few months

App updates sometimes add new features with new settings. Make a habit of checking your privacy settings every three or four months, and after any big update.

NOTE

For parents: most phones and app stores have family or parental control settings. They can filter content, require your approval before downloads and set time limits. Set them up together with your child and explain why, so they feel guided rather than spied on.

CHAPTER 4

Sharing photos safely

Photos say much more than we think. A single picture can show where you live, which school you go to and when your house is empty.

Before you post a photo, check the background

Do not post	Why
Your school uniform with a name badge or logo	Shows where you are every day
Your house number, gate or street sign	Shows where you live
Vehicle number plates	Can be traced to your family
Tickets, boarding passes, ID cards, report cards	Carry names, numbers and codes that can be misused
"We're off to Shimla for a week!" while away	Tells people your home is empty

Post holiday photos after you come home, not while you are away.

Many phone cameras can also save the place where a photo was taken inside the photo file itself. If you do not need this, turn off location in your camera settings, especially before sending photos to people you do not know well.

Other people's photos

Always ask before you post a photo of someone else, and remove it at once if they ask. Never share an embarrassing photo of a classmate, even "as a joke". Sharing a photo meant to shame someone is a form of bullying.

SAFETY

Never send private or undressed photos of yourself to anyone, even someone you trust completely. Once sent, you lose control of them, and they are often used for blackmail. Making or sharing such photos of anyone under 18 is a serious crime in India. If it has already happened, it is not too late: tell a trusted adult. You will be helped, not blamed.

Disappearing photos do not always disappear

Some apps promise that photos vanish after they are seen. The person receiving them can still take a screenshot, or simply photograph the screen with another phone. Treat every photo you send as if it could be kept forever.

Fake and edited images

Computer tools, including AI (artificial intelligence) apps, can now change photos or create fake ones that look real. A fake picture or video of a real person is sometimes called a deepfake. If someone makes or shares a fake image of you, remember that it is not your fault. Tell a trusted adult, save the evidence, report it to the app, and report it at cybercrime.gov.in.

REMEMBER

Keeping your account private and your photos limited to people you know makes it much harder for anyone to misuse them.

Cyberbullying and what to do

Cyberbullying is using phones, games or the internet to hurt, scare or embarrass someone, usually again and again. It can happen at any hour, follow you home and reach a large audience in minutes.

What cyberbullying looks like

- Mean or threatening messages and comments
- Spreading rumours or lies in a group
- Sharing embarrassing photos or videos
- Deliberately leaving someone out of a group chat or game
- Making a fake profile to pretend to be someone
- Posting someone's private messages to make fun of them

If you are being bullied

- 1. Do not reply or hit back.** Bullies want a reaction. Replying in anger can make things worse, and you could end up in trouble too.
- 2. Save the evidence.** Take screenshots that show the messages, the date and time, and the bully's username. Do not delete anything yet.
- 3. Block and report.** Every major app has a block button and a way to report abuse.
- 4. Tell a trusted adult:** a parent, a teacher or a school counsellor. You do not have to deal with it alone.
- 5. If there are threats** to hurt you, or someone shares private photos, report it to the police or at cybercrime.gov.in, with an adult's help.

REMEMBER

Being bullied is never your fault. Telling an adult is not "snitching" or weakness. It is the brave and sensible thing to do.

If you see someone being bullied

Be an upstander, a person who stands up for others, not a bystander who just watches. Do not like, share or laugh at the post. Send the person a private message of support: "That was not okay. Are you all right?" Report the post, and tell an adult.

Before you post, think

Sometimes people bully without meaning to. A comment that seems funny to you may hurt someone badly. "It was only a joke" does not undo the hurt. Before you post about anyone, ask yourself: "Would I say this to their face, in front of their parents?"

NOTE

For parents: signs that a child is being bullied include seeming upset after using the phone, avoiding school, deleting accounts, and changes in sleep or appetite. If your child tells you, stay calm, listen and thank them for telling you. Do not take the phone away as a punishment, because children who fear that stop telling. Work with the school to stop the bullying.

CHAPTER 6

Online friends and grooming warning signs

The internet lets you make friends who share your hobbies, from cricket to coding. Most of them are exactly who they say they are. But online, anyone can pretend. A "15-year-old girl from Pune" could be a 40-year-old man anywhere.

What grooming means

Grooming is when an adult builds a friendship and trust with a child or teenager in order to harm, use or abuse them. It happens slowly, so the child often does not notice it at first.

Warning signs

Be careful if an online friend:

1. Gives you a lot of attention and compliments, and says nobody understands you like they do.
2. Sends gifts, such as game credits, mobile recharges or money.
3. Asks you to keep your friendship secret from your parents.
4. Wants to move from a group or game chat to a private chat app.
5. Asks personal questions about your body, your family or when you are alone.
6. Asks for photos, especially private ones, or sends you such photos.
7. Tries to turn you against your parents or friends.
8. Wants to meet you in person, alone.
9. Gets angry, or threatens you, when you say no or try to stop talking.

What to do

- **Stop replying**, but do not delete the chat. Take screenshots first.
- **Block and report** the account on the app.
- **Tell a trusted adult** straight away, even if you broke a rule earlier. Your safety matters far more than the rule.
- **Never meet an online friend alone.** If an older teenager truly wants to meet someone they know only online, a parent must know, go along, and the meeting must be in a busy public place.

SAFETY

If someone threatens to share your photos unless you send money or more pictures, do not pay and do not send anything. Stop replying, save the evidence and tell an adult at once. Report it at cybercrime.gov.in. In an emergency, call 112. The child helpline is 1098.

NOTE

For parents: talk about online friends the same way you talk about friends at school. Ask who your child chats with and what games they play, with curiosity, not suspicion. A child who expects to be scolded will hide things; a child who expects to be helped will come to you early.

CHAPTER 7

Fake news and checking facts

Fake news, or misinformation, is false or misleading information that is shared as if it were true. Some people spread it on purpose to fool, scare or anger others. Many more spread it by accident, because they forwarded something without checking.

Fake news spreads fast because it is designed to make us feel something strongly: shock, fear, anger or excitement. When we feel strongly, we forward before we think.

Six steps before you share

- 1. Stop.** If a message makes you feel a strong emotion, slow down. That is exactly when to check.
- 2. Ask who is saying it.** Is there a name, a newspaper, an official website? "Forwarded as received" means nobody is taking responsibility.
- 3. Look for other sources.** If something big has really happened, trusted newspapers and news channels will also report it.
- 4. Check pictures.** Old photos are often reused with new false stories. Many search apps let you search with a photo to see where else it has appeared, and when.
- 5. Check the date.** Old news is often shared again as if it happened today.

6. Watch for warning words. "Share before it is deleted!", "The media won't tell you this", lots of capital letters and exclamation marks are all warning signs.

EXAMPLE

One evening, a message in Aditya's class group says: "All schools in the district closed tomorrow due to heavy rain. Order of the District Collector." It has no link and no date. Aditya checks his school's official notice and the district administration's official account. There is no such order, so he does not forward it, and he tells the group it seems to be fake.

Fact-checkers

Fact-checking groups investigate viral claims and publish what is true. The government's PIB Fact Check unit checks false claims about the central government. Checking with one or two trusted sources takes a minute and can stop a rumour.

DID YOU KNOW

AI tools can now copy a person's voice or face in a video. A clip of a famous person saying something shocking may be fake. Look for a trusted news report before you believe it.

Health rumours

Messages about "miracle cures" or dangerous foods are among the most common fake forwards. Never try a cure from a forwarded message. Ask a doctor.

NOTE

For parents: children copy what they see. If you check before you forward, and say so out loud ("Let me check this before I share it"), your child learns the habit too.

Gaming safety and in-app purchases

Games can be great fun and can build teamwork, planning and quick thinking. A few simple habits keep gaming safe and stop it from costing your family money.

Age ratings

Every game in an app store shows an age rating, which tells you the youngest age it is suitable for. Ratings consider violence, scary scenes, language and chatting with strangers. Choose games rated for your age, and ask a parent before downloading anything else.

In-app purchases

Many "free" games make money through in-app purchases: real money spent inside the game on coins, gems, skins, passes or extra lives. Some games sell loot boxes, mystery rewards you pay for without knowing what you will get. Loot boxes work like a lucky draw and can make players spend more and more.

EXAMPLE

Kabir, aged 12, played on his mother's tablet, where her card was saved in the app store and purchase approval was switched off. In one week, he spent ₹2,400 on gems, thinking they were part of the game. The family then set the store to ask for a password or fingerprint before every purchase, and Kabir now has a fixed monthly limit agreed with his parents.

Free-reward scams

Websites and videos that promise "free diamonds" or "free skins" usually want your game login. Once they have it, they take over your account and sell it. Never enter your game username and password anywhere except inside the game itself or on its official website.

Chatting while gaming

Many games let you talk to other players by voice or text.

- Never share your real name, school, city, phone number or photos.
- Use the game's settings to allow chat with friends only.
- Mute, block and report anyone who is rude, asks personal questions or makes you uncomfortable.
- Remember the grooming warning signs. Gifts of game credits from a stranger are a red flag (a warning sign).

Money games

Stay away from any game or app that asks you to put in money to win more money. These are a form of gambling. In 2025, India passed a law banning online money games, but illegal apps and websites still try to attract players, especially young people.

TIP

Set a timer when you start playing, and stop when it rings. Finish homework first, and keep gaming out of the hour before bed.

CHAPTER 9

Phishing and scams

Phishing (said like "fishing") is a trick to make you give away a password, an OTP or bank details, or to click a harmful link. The scammer "fishes" with a fake message and waits for someone to bite. It can come by SMS, email, WhatsApp, a social media message or a phone call.

How to spot a phishing message

1. **It rushes you:** "Your account will be blocked in 24 hours!"

2. **It offers something too good to be true:** "You have won a lottery of ! 25 lakh!"
3. **It asks for secrets:** an OTP, a PIN, a password or card details.
4. **The link looks odd:** spelling mistakes, extra words or strange endings in the web address.
5. **It comes from an unknown sender,** or from a friend's account that suddenly writes in a strange way.

SAFETY

Never install an app sent to you as a file in WhatsApp, SMS or email (such a file often ends in ".apk"), even if it looks like a wedding invitation or a bill. Install apps only from your phone's official app store.

UPI facts every family should know

- You **never** need to enter your UPI PIN to **receive** money. A PIN is only for paying.
- Scanning a QR code is for **paying**, not for receiving. If someone says "scan this to receive your refund", it is a scam.
- A payment request that you approve with your PIN takes money out of your account. Read every request carefully, and never approve one you did not expect.

Common scams

Scam	What happens
Fake customer care	You search online for a helpline and call a scammer's number, who asks for your OTP or asks you to install an app.
KYC update	A message says your bank or SIM will be blocked unless you "update KYC" through a link.

Scam	What happens
Electricity bill	An SMS says your power will be cut tonight unless you call a number and pay.
Courier or parcel	A caller says a parcel in your name contains illegal items and you must pay to clear it.
"Digital arrest"	Fake police or officers on a video call say you are under arrest and must transfer money. There is no such thing as a "digital arrest"; real police never arrest anyone or collect money over a video call.
Fake job or task	You are paid small amounts for simple tasks, then asked to invest money for bigger ones.

If you have been cheated

- 1. Call 1930**, the national cyber crime helpline, at once. The sooner you report, the better the chance of stopping the money.
- 2. Report it at cybercrime.gov.in.**
- 3. Call your bank** to block your card or account if needed.
- 4. Change your passwords**, starting with email.
- 5. Keep all evidence:** screenshots, phone numbers and transaction IDs.

You can also report suspected fraud calls and messages through the government's Sanchar Saathi service.

CHAPTER 10

Screen time and sleep

Screens are not the enemy. We use them to learn, to talk to family and to relax. The problem starts when screen time pushes out the things our bodies and minds need: sleep, exercise, real conversations and homework.

How much sleep do you need?

Sleep experts advise that most children aged 6 to 12 need about 9 to 12 hours of sleep a night, and most teenagers aged 13 to 18 need about 8 to 10 hours. Sleep is when your body grows and repairs itself, and when your brain stores what you learned during the day.

Bright screens and exciting videos or games just before bed make it harder to fall asleep. Notifications at night wake you up. A tired student finds it harder to concentrate, remember and stay cheerful.

Healthy screen habits

- 1. Switch off screens an hour before bed.** Read a book, talk with family or listen to calm music instead.
- 2. Charge phones outside the bedroom** at night. Use a simple alarm clock if you need one.
- 3. Turn off unneeded notifications**, so your phone does not keep pulling you back.
- 4. Use the built-in screen-time tools** on your phone to see how long you spend on each app, and to set limits.
- 5. Move every day.** The World Health Organization advises that children and teenagers get an average of at least 60 minutes of active play or exercise a day.

TIP

Rest your eyes with the 20-20-20 habit: every 20 minutes, look at something about 20 feet (6 metres) away for 20 seconds. Hold the screen at a comfortable distance and sit up straight.

Signs of too much screen time

- Feeling angry or upset when asked to stop
- Losing interest in friends, sport or hobbies you used to enjoy

- Falling marks or unfinished homework
- Feeling tired every morning

If you notice these signs in yourself, it is time to cut down. Start small: one screen-free hour a day, then two.

EXAMPLE

Meher, in class 7, made this plan for a school day with her parents.

Time	Activity
After school	Snack, then one hour of play outside
Evening	Homework first, with the phone in another room
After homework	Up to one hour of games or videos
Dinner	Screen-free, for the whole family
One hour before bed	Phone on charge in the living room; reading

NOTE

For parents: children notice our habits. Make meal times and the hour before bed screen-free for the whole family, including adults. Shared rules are much easier to follow than rules only for children.

CHAPTER 11

Reporting and your family agreement

Knowing where to go for help is the most important safety skill of all. Problems online get worse when they are hidden and better when they are reported early.

Where to get help

Problem	Where to go
Someone is in danger right now	Call 112, the national emergency number
A child needs help or protection	Call 1098, the child helpline
Money has been stolen online	Call 1930 at once, then report at cybercrime.gov.in
Bullying, threats, fake profiles, blackmail, sharing of private photos	Report at cybercrime.gov.in , which has a section for crimes against women and children; or go to your nearest police station
A rude or harmful post or account	Use the app's own report button

Save evidence first

Before you block anyone or delete anything, collect the evidence: screenshots showing messages, dates and times; the person's username or profile link; phone numbers; and, for money fraud, transaction IDs and bank messages. Keep them in a folder. Police and apps can act much faster when the evidence is clear.

REMEMBER

Reporting is not "getting someone into trouble". It protects you, and it may protect the next child the same person targets.

Your family agreement

A family agreement is a set of simple rules that children and parents make together and promise to follow. Rules you help to make are easier to keep. Copy this template into a notebook, fill in the blanks together, sign it and put it somewhere everyone can see. Review it every six months.

Our family's online agreement

Children's promises:

1. I will keep my passwords secret from everyone except my parents, and I will never tell anyone an OTP.
2. I will keep my accounts private and accept only people I know in real life.
3. I will not share my address, school, phone number or location online.
4. I will ask before posting photos of other people.
5. I will never meet an online friend without my parents knowing and coming along.
6. I will tell a parent if anything online makes me feel scared, sad or uncomfortable.
7. On school days, my screen time for fun is hours, and on holidays hours.
8. Phones are charged outside bedrooms from pm.

Parents' promises:

1. We will listen calmly, and we will not punish you for telling us about a problem.
2. We will ask before posting photos of you.
3. We will follow the screen-free meal and bedtime rules too.
4. We will learn about the apps and games you use.

Signed (child): Signed (parents): Date:

CHECK YOURSELF

Practice questions

1. What is a digital footprint?
2. What is the difference between an active and a passive footprint?

- 3.** Describe the hoarding test.
- 4.** Give two features of a strong password.
- 5.** Why is your email password the most important one to protect?
- 6.** What is two-step verification, and why does it help?
- 7.** Who should you tell a login or payment OTP to?
- 8.** Name three privacy settings you should check on every app.
- 9.** Why should a torch app not have permission to read your contacts?
- 10.** Name three things to check in the background of a photo before you post it.
- 11.** Why should you post holiday photos after you come home?
- 12.** Give the five steps to follow if you are being cyberbullied.
- 13.** What is an upstander?
- 14.** List four warning signs of grooming.
- 15.** What should you do if someone threatens to share your photos unless you pay?
- 16.** Give four steps to check a message before you forward it.
- 17.** What is an in-app purchase, and how can a family stop unplanned spending?
- 18.** Why should you never enter your game login on a "free diamonds" website?
- 19.** Do you need to enter your UPI PIN to receive money?
- 20.** What is the "digital arrest" scam, and what is the truth about it?
- 21.** Which number should you call at once if money has been stolen online?
- 22.** How many hours of sleep do most teenagers need?
- 23.** Why do family agreements work better when children help to make them?

Answers

1. The trail of everything you do online, plus what others post about you.
2. An active footprint is what you share on purpose; a passive footprint is collected without you noticing, such as your location and the sites you visit.
3. Imagine your post on a giant hoarding at a busy crossing with your name and photo. If you would not be happy for everyone to see it, do not post it.
4. Any two of: it is long (at least 12 characters), hard to guess, and used for only one account.
5. Because whoever controls your email can reset the passwords of your other accounts.
6. It needs a second proof, such as a code on your phone, besides your password, so a stolen password alone is not enough to log in.
7. No one. Banks, game companies and police never ask for it.
8. Any three of: a private account, your followers list, who can message or tag you, hiding your phone number and email, location sharing.
9. A torch app does not need contacts to work, so the permission could only be used to collect your data.
10. Any three of: a uniform with a badge or logo, your house number or street sign, vehicle number plates, tickets or ID cards.
11. Posting while away tells people your home is empty.
12. Do not reply; save evidence; block and report; tell a trusted adult; report threats to the police or at [cybercrime.gov.in](https://www.cybercrime.gov.in).
13. Someone who supports a person being bullied and reports it, instead of just watching.
14. Any four of: lots of attention and compliments, gifts, asking for secrecy, moving to a private chat, personal questions, asking for photos, turning you against family, wanting to meet alone, threats.
15. Do not pay or send anything; stop replying; save evidence; tell an adult; report at [cybercrime.gov.in](https://www.cybercrime.gov.in).

- 16.** Any four of: stop; ask who is saying it; look for other sources; check pictures; check the date; watch for warning words.
- 17.** Real money spent inside a game.
Families can make the store ask for a password or fingerprint before every purchase and agree a spending limit.
- 18.** Such sites usually steal the login and take over the account.
- 19.** No. A UPI PIN is only needed to pay.
- 20.** Fake officers on a video call claim you are under arrest and demand money. There is no such thing as a digital arrest; real police never arrest or collect money over a video call.
- 21.** 1930, the national cyber crime helpline.
- 22.** About 8 to 10 hours a night.
- 23.** People are more likely to keep rules they helped to make.

WORD LIST

Glossary

Age rating

a label showing the youngest age a game or app is suitable for.

Authenticator app

an app that shows a fresh login code, usually every 30 seconds, for two-step verification.

Cyberbullying

using phones, games or the internet to hurt, scare or embarrass someone.

Deepfake

a fake photo, video or voice recording made with computer tools to look real.

Digital footprint

the trail of everything you do online.

Evidence

screenshots, usernames, numbers and other records that show what happened.

Fake news

false or misleading information shared as if it were true.

Grooming

when an adult builds trust with a child in order to harm or abuse them.

In-app purchase

real money spent inside an app or game.

Loot box

a paid mystery reward in a game.

Misinformation

false information, whether shared on purpose or by mistake.

Notification

an alert from an app that appears on your screen.

OTP

a one-time password, a short code sent to your phone to confirm who you are.

Passphrase

a password made of several random words joined together.

Permission

access an app asks for, such as to your camera or location.

Phishing

a fake message designed to steal passwords, OTPs or bank details.

Privacy settings

the controls that decide who can see and contact you.

Screenshot

a picture of what is on a screen.

Two-step verification

logging in with a password plus a second proof, such as a code.

Upstander

a person who stands up for someone who is being bullied.

UPI PIN

the secret number used to approve a UPI payment.



Gurukul Technicals Institute

Computer education institute in Delhi, with authorised member centres, robotics classes and science projects, working models and DIY kits.

COURSES

Computer & Office Skills · Accounting & Business Software · Programming & Web Development · Design & Digital Skills · Hardware & Networking · Robotics & Coding · Other Programmes

PROJECTS AND KITS

Ready-made school projects · DIY and STEM kits · Robotics and coding · Components and spares · Engineering projects

CONTACT

Head office: A-10, Chief Commissioner Colony, opposite Rana Pratap Bagh, Delhi 110007

Phone: 011 2721 1512 · **Mobile and WhatsApp:** +91 97116 99511

Email: engineergurukul@yahoo.co.in

Website: engineergurukul.com · **Instagram:** [@science_projects_club](https://www.instagram.com/science_projects_club)

More free ebooks for computer courses, robotics and science projects: engineergurukul.com/resources/ebooks/

Free to read, print and share. Not for sale.