

**Previously – What the Group Has Learned So Far**

Ch.1: Aryan recovered from a UPI hack using strong passwords & 2FA. | **Ch.2:** Naman learned to manage digital tracking and app permissions. | **Ch.3:** Kavya lost a scholarship due to an old post — rebuilt using the THINK Rule. | **Ch.4:** Rohan was cyberbullied for reporting cheating — the group became upstanders and reported to the Cyber Crime Cell. All five are now Cyber Safety Ambassadors. **In Chapter 5,** they encounter a new threat — one that targets trust itself.

Chapter 5 – Grooming & Sextortion Awareness**Key Terms – Your Safety Dictionary****Grooming**

A process where someone **builds trust over time** to gain access, lower a person's guard, and eventually manipulate or exploit them — online or offline.

**Sextortion**

When someone **threatens to share** intimate images or information unless the victim pays money, sends more images, or does something they don't want to do.

**Secrecy Pressure**

When someone insists a relationship or conversation must be kept **hidden from parents, teachers, or friends** — a major warning sign of exploitation.

Breaking Story – Read This First!**THE HIMACHAL HERALD**

Monday, 16th March 2026 · Student Safety Edition

△ SPECIAL REPORT: SHIMLA STUDENT TARGETED THROUGH ONLINE "FRIENDSHIP" – FAMILY SEEKS HELP △

CLASS 10 STUDENT FROM SHIMLA DECEIVED BY UNKNOWN PERSON POSING AS PEER — WEEKS OF MESSAGES PRECEDED THE THREAT

By Our Education Correspondent, Shimla, HP

Meera (name changed), a Class 10 student from Shimla, began receiving messages from someone presenting themselves as a fellow Class 10 student from Delhi — "Rishabh." Over several weeks, Rishabh sent encouraging messages, shared personal stories, and asked Meera to keep the friendship private. "He said his friends wouldn't understand," Meera later told counsellors.

After weeks of building trust, Rishabh asked Meera to share a photograph. When she hesitated, he said: "Don't you trust me? I thought we were close."

Meera's older friends — Kavya's group — noticed she had become withdrawn and anxious. When they gently asked, she showed them the messages. Aryan recognised the pattern immediately: "This is grooming. Step by step."

What experts say: "Grooming takes time because trust takes time. By the time a young person realises something is wrong, they often feel too ashamed or too scared to speak up." — Dr. Anita Sharma, Child Safety Expert, NIMHANS

Meera's family has filed a complaint. The case is under investigation by the HP Cyber Crime Cell.

△ It is never the victim's fault. Groomers are skilled manipulators — they choose their targets carefully and deliberately. Speaking up is the bravest thing you can do.

**Pause & Think!**

Before you read any further — notice how Meera's story started. Not with a threat. Not with something obviously wrong. It started with what felt like a **normal online friendship**. This is the most important thing to understand about grooming: by the time something feels clearly wrong, the trap has often already been set. The goal of this chapter is not to make you afraid of every online conversation — it is to make you **informed enough to tell the difference**.

Read & Reflect**After Reading Meera's Story****RQ1.**

Rishabh asked Meera to keep the friendship secret. Why is secrecy in an online relationship — especially with someone you have never met in person — a significant warning sign?

The Grooming Stages – How Trust Is Weaponised

Grooming is not a single event — it is a **deliberate process**. Understanding each stage helps you spot it early and protect yourself and others.



Stage 1: Target

The groomer identifies a vulnerable person — often someone who seems lonely, seeking attention, or going through a hard time.



Stage 2: Build Trust

Excessive attention, compliments, gifts (real or digital). "You're so mature for your age." Creates a sense of being special.



Stage 3: Isolate

"Don't tell your parents — they won't understand." Gradually separates the target from trusted people who might notice.



Stage 4: Desensitise

Slowly introduces inappropriate content, requests, or conversations — testing boundaries incrementally until the target feels normalised.



Stage 5: Exploit & Control

Uses what was shared — images, secrets, feelings — to threaten, manipulate, or demand more. The trap is now set.



Pause & Think!

Notice that Stage 1 to Stage 4 can feel completely **normal** — even good. Someone being kind, paying attention, making you feel special. This is exactly what makes grooming so dangerous and why it is **never the victim's fault**. A skilled manipulator is specifically designed to feel safe. The warning signs are not always obvious in the moment — but they are easier to spot when you know what to look for. **Knowing this is your protection.**

Red Flags vs Green Flags – How to Tell the Difference

Red Flags – Warning Signs

- ✗ Asks you to keep the friendship or conversation secret
- ✗ Claims to be exactly your age with very similar interests
- ✗ Moves very fast — "I feel like I've known you forever"
- ✗ Says your parents or friends "wouldn't understand"
- ✗ Asks for photos — especially when you seem hesitant
- ✗ Sends you gifts, data, game credits, or money
- ✗ Makes you feel guilty for not sharing: "Don't you trust me?"
- ✗ Suggests meeting in person alone, or switching to private apps

Green Flags – Healthy Online Relationships

- ✓ You can talk about this person openly with your parents
- ✓ They respect it when you say no or change the subject
- ✓ The relationship doesn't feel rushed or intense
- ✓ They never ask you to keep things secret
- ✓ They don't ask for photos or personal information
- ✓ You feel comfortable — not confused, guilty, or anxious
- ✓ Your friends and family know they exist
- ✓ They never make you feel like you owe them something

Activity 1

Spot the Stage – Meera's Story

Each message below is from the newspaper story. Write which Grooming Stage (1–5) it matches and which Red Flag it shows.

Rishabh's message or action	Stage (1–5)	Red Flag it shows
"You're so mature for your age — different from other girls."	<input type="text"/>	<input type="text"/>
"Don't tell your friends about us — they won't understand."	<input type="text"/>	<input type="text"/>
"Don't you trust me? I thought we were close."	<input type="text"/>	<input type="text"/>
Sent Meera a ₹200 game top-up as a "gift" after two days.	<input type="text"/>	<input type="text"/>

Q1a.

Aryan says Meera's situation is "textbook grooming." Which single stage do you think was the most dangerous turning point — and why?

Q1b. Match the term to its meaning — write the letter in the box

TERMS

1 Trust Building	<input type="checkbox"/>
2 Isolation	<input type="checkbox"/>
3 Desensitisation	<input type="checkbox"/>
4 Sextortion	<input type="checkbox"/>

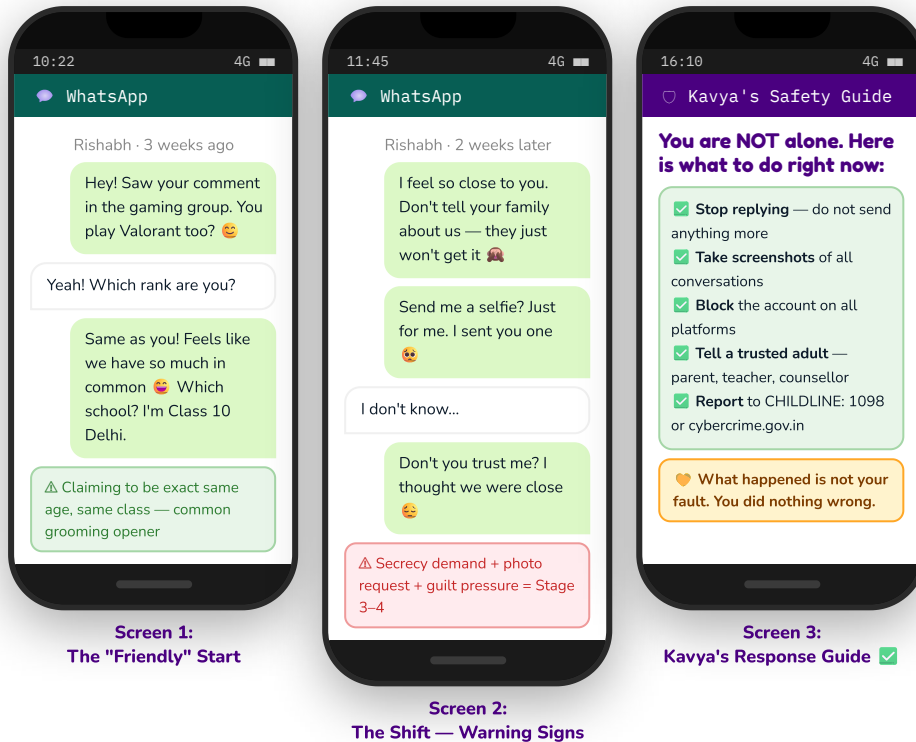
MEANINGS

A. Threatening to share images unless demands are met
B. Gradually introducing inappropriate topics to lower boundaries
C. Using gifts, attention, and compliments to make someone feel special
D. Cutting a person off from parents and friends using secrecy

Answers: 1–C, 2–D, 3–B, 4–A

What Meera's Phone Showed – Three Moments in the Conversation

Screen 1 is how Rishabh first approached Meera. Screen 2 is the shift — when his true intent appeared. Screen 3 is what Kavya showed Meera after she opened up.



Pause & Think!

Look at Screen 2 carefully. Rishabh used three tactics in the same conversation: **demand for secrecy, a photo request, and guilt when refused**. Notice that Meera's instinct was correct — she hesitated and said "I don't know." **That hesitation was her instinct protecting her.** One of the most important things you can do is trust that feeling. If something feels wrong online — even if you can't explain why — it probably is.

Activity 2

Analyse the Three Screens

Q2a.

Screen 1 looks completely harmless. List **TWO** specific things in Screen 1 that are actually early grooming tactics — and explain why each one is a warning sign:

What looks harmless but isn't	Why it's actually a warning sign
1.	
2.	

Q2b.

Meera said "I don't know" when asked for a photo. Rishabh immediately responded with guilt. Why is using guilt to override hesitation a serious manipulation tactic — and what should Meera have done next?

Q2c.

Screen 3 shows Kavya's safe response guide. Which step do you think is the most important — and why? Is there anything you would add?

Q2d. Odd One Out – circle the one that does NOT belong, then explain why

The odd one out is: _____ Because: _____

Story – The Group Responds

Scene 1 – School Corridor, Delhi · Meera Has Just Shown Kavya the Messages



NEW
Meera

I feel so stupid. I should have known. Maybe it is my fault for talking to him in the first place.
hands shaking



Kavya

Stop. Listen to me. **This is not your fault.** He studied you, chose you deliberately, and used your trust against you. That is on him — not you. You did nothing wrong by wanting a friend.



Aryan

I recognise this pattern exactly. Grooming. He built trust first, then asked for something. The moment he said "don't tell anyone" — that was the clearest sign. **We need to screenshot everything before he deletes his account.**



Priya

Meera, you showed us. That was the hardest and most important thing you could have done. From here we go together. You are not handling this alone.



Naman

In Chapter 2 I felt ashamed that I was being tracked without knowing. I thought I should have noticed. But the whole point is that it was designed so you *wouldn't* notice. Same here. This is on him.

Pause & Think!

Notice the roles in this scene. Kavya speaks to the *shame*. Aryan speaks to the *evidence*. Priya speaks to the *support*. Naman connects it to his own experience of feeling foolish. Together, they cover everything Meera needs in this moment. **This is what a real support network looks like.** You don't have to say the perfect thing — you just have to show up, listen, and not make it worse by blaming the person who was hurt.

Activity 3

Story Analysis – What Each Character Brings

Q3a.

Meera's first reaction is to blame herself: "Maybe it is my fault." This is called **self-blame** — very common in grooming and sextortion cases. Using the characters' responses, write **TWO** reasons why Meera is **NOT** at fault:

Reason 1 (from Kavya's response):

Reason 2 (from Naman's response):

Q3b.

Aryan says: "The moment he said 'don't tell anyone' — that was the clearest sign." Why is the demand for secrecy such a definitive warning signal in online relationships?

Q3c. Tick ALL that apply

Which of the following are reasons why a victim might choose to stay silent rather than tell a trusted adult? Tick all that apply — then circle the **ONE** you think is most powerful:

- "I feel ashamed — I should have known better."
- "I don't want my parents to blame me or take away my phone."
- "He said he'd make things worse if I told anyone."
- "I thought it would stop on its own if I ignored it."
- "I didn't know there was a law that could actually help me."
- "I was scared no one would believe me."

What Grooming and Sextortion Can Actually Cost



Mental Health Impact

Anxiety, depression, shame, and isolation are the most common effects. Victims often withdraw from school, friends, and family before seeking help.



Academic Disruption

Fear of going to school, difficulty concentrating, and drop in performance. Many victims struggle silently for months before adults notice.



Family Strain

Shame often prevents victims from telling family. When they do, families may react with anger or blame — making it harder to heal.



Loss of Safety Online

Victims may avoid digital spaces entirely or develop distrust of online connections — affecting education and social life long-term.



Legal Consequences for Perpetrators

Grooming and sextortion are criminal offences. Perpetrators face serious legal consequences — but only when cases are reported.



Recovery Is Possible

With the right support — counselling, trusted adults, and legal help — survivors recover fully. **Speaking up is the first step.**

Let's Assume – A Data Interpretation Exercise

The figures below are discussed in various child safety studies. For this activity, **treat them as assumptions** to explore what they might mean — not as verified facts.

1 in 3

young people may receive an unwanted sexual message or approach online before age 18

70%

of grooming cases may begin on mainstream platforms — games, social media, study groups

6 wks

average time before a groomer may make a harmful request after first contact

1 in 5

victims of sextortion may never tell anyone — shame is the biggest barrier to getting help



Pause & Think!

Look at the "1 in 5" figure. If one in five victims never tells anyone — that means in a class of 30 students, there may be someone silently carrying this right now. The reason they stay silent is almost always **shame and self-blame** — the feeling that they should have known better. But as Kavya told Meera: the groomer chose them deliberately, built trust carefully, and exploited it. **There is nothing to be ashamed of. There is only something to report.**

Activity 4

Data Decoder – What Do These Numbers Mean?

Q4a.

The "70%" figure says grooming often starts on mainstream platforms — not dark websites. Does this surprise you? How does it change how you think about messages from strangers on Instagram or gaming apps?

Q4b.

The "1 in 5 never tell anyone" figure links directly to shame. What would you say to a friend who said: "I can't tell anyone — they'll think it's my fault"? Write 2–3 sentences you would actually say:

Q4e. MCQ – circle the correct answer

Which of the following best describes **WHY** grooming is hard to recognise in its early stages?

- (A) The groomer immediately asks for personal information
- (B) The early stages look like normal kindness, attention, and friendship
- (C) The victim is always someone who ignores safety rules
- (D) Groomers always use fake names and obvious false identities from the start

Q4c.

The "6 weeks" figure says a groomer may wait an average of 6 weeks before making a harmful request. Why does this delay make grooming harder to recognise — and how does it relate to why victims often say "I should have noticed earlier"?


Q4d.

Looking at all four data points together — 1 in 3 approached online, 70% on mainstream apps, 6 weeks average, 1 in 5 never tell — what do they tell you about where the biggest gap is in how we currently respond to this problem? Is it awareness, support, or something else?

The 5-Step Safe Response Framework

Aryan writes these steps on a piece of paper for Meera. Follow them in order — every step matters.


1



Stop Responding

Do not reply, send more images, or comply with any demands. Every response gives the person more power.


2



Screenshot Everything

Capture all messages, profiles, usernames, and timestamps before blocking. This is your evidence.


3



Block & Report

Block the account on every platform. Use the "Report" function — this flags the account to the platform.


4



Tell a Trusted Adult

Parent, teacher, school counsellor — someone you trust. You do not need to handle this alone.

5



File a Report

Report to CHILDLINE (1098), cybercrime.gov.in, or the National Commission for Protection of Child Rights (NCPCR).

Pause & Think! Look at Step 1: **Stop Responding**. This feels counterintuitive — your instinct is to defend yourself, explain, or negotiate. But every message you send gives the perpetrator more material and more power over you. Silence is your first act of taking control back. Step 2 — **Screenshot Everything** — is equally critical. Without evidence, reporting is harder. With it, the case against the perpetrator becomes much stronger. **These two steps together change the balance of power immediately.**

Who to Call – Helplines & Resources

1098

CHILDLINE India

Free, 24/7, confidential helpline for children in distress. Available across India. Hindi, English, and regional languages.

cybercrime.gov.in

National Cyber Crime Reporting Portal

File complaints about online grooming, sextortion, and image-based abuse. Under Ministry of Home Affairs, Govt. of India.

iCall

iCall – TISS

Psychosocial helpline by Tata Institute of Social Sciences. Free counselling for mental health support. 9152987821.

Indian Laws That Protect You

POCSO Act 2012

Protection of Children from Sexual Offences. Online grooming of minors (under 18) is a criminal offence — up to 5 years imprisonment.

IT Act Sec 67A & 67B

67A: sexually explicit material online, 67B: sexual content involving minors specifically — up to 5 years, first offence.

IPC Sec 383

Definition of extortion — putting someone in fear and dishonestly inducing them to deliver property or valuables. Foundation of sextortion cases.

IPC Sec 384 & 385

Punishment for extortion (384) and putting someone in fear of injury to commit extortion (385). Directly covers sextortion demands.

Important: The law is on your side. Reporting is protected — you are the victim. The perpetrator faces consequences, not you.

Quick Check

MCQ – Before You Sort

Q. Meera has just received a sextortion threat. What is the **FIRST** thing she should do?

- (A) Reply to the person explaining she will report them
- (B) Delete all messages immediately so no one sees them
- (C) Stop responding and screenshot all conversations as evidence
- (D) Pay what they ask so they will stop threatening her

Story – Priya Explains Sextortion

Scene 2 – Later That Day · The Group Explains What Sextortion Is and Why Paying Never Helps



He said if I don't send more photos, he will share what I already sent with my school contacts. I'm scared. Should I just... give him what he wants so he stops?

No. That is called sextortion — and paying or complying never makes it stop. It tells him it works. He will ask for more. The only way out is to stop responding completely and report immediately.



And if he does share something — which often they don't, it's a bluff to control you — the law protects you, not him. **He is committing a crime under the IT Act and IPC 384.** You are the protected party here.

The screenshots you took? That is your evidence. His username, the timestamps, the content of the threats — all of it. We file the report together. Right now.



Pause & Think!

Priya's key point: **paying or complying with a sextortion demand never makes it stop — it proves it works.** This is one of the most important things to understand about sextortion. The demand will escalate. The only effective response is to stop contact completely, preserve evidence, and report. If someone you know is facing this situation — the kindest thing you can do is tell them: the law is on their side, and they are not alone.

Activity 6

Sextortion – Myths vs Facts

Read each statement. Tick whether it is a Myth or a Fact — then write a correction or explanation for each.

Statement	Myth	Fact	Correction / Explanation
"If I pay, they will stop."	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
"If this happens to me, it is my fault for sharing."	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
"Once I block them, the threat disappears."	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
"Reporting to the police will make things worse for me."	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>
"The person threatening me is always a stranger."	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text"/>

Q6a.

Which of the five myths above do you think is the most dangerous — because believing it could cause the most harm to a victim? Give a reason:

Q6b. True / False – circle your answer

T F Complying with a sextortion demand makes the perpetrator stop.

T F Grooming victims are targeted because of something they did wrong.

T F Reporting online exploitation protects the victim, not the perpetrator.

T F A groomer can be traced even if they use a fake name and profile.

Q6c.

Meera said: *"I kept tolerating it because telling my parents felt scarier than the threat itself."* In your own words, explain how staying silent — even when someone feels deeply unsafe — affects their mental health over time, and why it is critical that schools create space for students to speak up without fear of being judged:

Deep Analysis – Two Cases

Priya shares two patterns from cases reported across India. Read carefully and answer the questions that follow.

Case A – "The Gaming Friend" (Class 9, Delhi)

Ravi, a Class 9 student from Delhi, met "Alex" in an online game. Alex was generous — sending him rare in-game items and offering to help him rank up. Over two months, Alex moved the conversation to WhatsApp. He shared fake personal problems and asked Ravi to keep the friendship private. One evening, Alex sent Ravi an inappropriate image without warning. When Ravi was shocked and said he would report it, Alex said: "Go ahead — but I'll tell your parents you asked for it. I have screenshots." Ravi was terrified and said nothing for three weeks.

Contact began via
Online gaming — a mainstream platform

Trust-building used
In-game gifts + fake personal stories

Control tactic used
False accusation threat + shame



Pause & Think!

Ravi's case adds something new: the **false accusation threat**. Alex said "I'll tell your parents you asked for it." This is a deliberate tactic — designed to make the victim feel that speaking up will make their situation worse, not better. But think about it carefully: the screenshots Ravi has are dated, timestamped, and show who sent what first. **Evidence does not lie**. The law looks at what actually happened — and what actually happened was done to Ravi, not by him.

Challenge Activity A

Analyse Ravi's Case

CA1.

Alex used in-game gifts as part of the trust-building process. Why are gifts — whether physical or digital — a grooming tactic, and why do they create a sense of obligation in the recipient?

CA2.

Alex threatened: "I'll tell your parents you asked for it." This is a false accusation threat — designed to make Ravi feel that speaking up will make things worse. Build arguments for BOTH sides, then give your own judgement:

Why Ravi might believe the threat:

Why reporting is still the right action:

My judgement:

CA3.

At which Grooming Stage (1–5 from Page 2) did Alex cross from trust-building into exploitation — and what was the specific action that marked that crossing?



Apply the Laws – Which Applies to Ravi's Case?

Using the three laws from Page 6, identify which law applies to each of Alex's actions and explain why:

Sending Ravi an unsolicited inappropriate image:

Threatening to fabricate evidence unless Ravi complies:

Case B – "The Classmate's Account" (Class 11, HP)

Sana, a Class 11 student from Solan, HP, received a follow request from an account with her classmate's name and photo. Believing it was her friend's new account, she accepted and began chatting. The account sent affectionate messages and eventually asked her to share a private photo "since we already know each other." Sana shared one — and immediately received a screenshot of it with a demand: "Pay ₹3,000 or I send this to your class group." Sana checked with her actual classmate, who confirmed her account had been cloned without her knowledge. Both girls were now victims.

Deception method

Cloned account using real classmate's identity

Trust exploit used

Pre-existing real-world relationship assumption

Outcome

Two victims — the target AND the impersonated classmate

Challenge Activity B

Analyse Sana's Case

CB1.

This case shows that grooming can exploit trust in *existing* relationships — not just new strangers. What specific verification step could Sana have taken before accepting the follow request that would have immediately revealed the deception?

CB2.

Sana's classmate is also a victim — her identity was stolen and used to harm someone else. What are TWO things the classmate should do immediately upon discovering her account was cloned?

Action 1:

Action 2:



Pause & Think!

Sana's case introduces something that Ravi's and Meera's cases didn't: the cloned identity. This means grooming can now begin by **disguising itself as a known, trusted person**. The safety check is simple but vital: if you receive a new follow request or contact from someone you already know, **verify through a different channel first** — call them, text their known number, or ask them in person. A two-second check can prevent everything that followed in Sana's case.

Activity 7

Design Your Personal Safety Protocol

After studying all three cases — Meera, Ravi, and Sana — write your own rules for staying safe online. Be specific and honest.

Warning signs I will now look out for:

What I will do if it happens to me:

Who I will tell (trusted adult in my life):

What I will say if a friend comes to me:

Q7e.

Across all three cases — Meera, Ravi, and Sana — each victim spent time in silence before anyone found out. Looking back at the data (1 in 5 never tell), how do you think your school could make it *easier* for students to speak up — without shame and without fear? Write one specific, realistic change:

I will not stay silent — for myself or for someone I care about. Sign: _____ Date: _____

Pause & Think!
You have now studied three different grooming and sextortion scenarios — Meera, Ravi, and Sana. Each one started differently, but all three had something in common: the perpetrator relied on **silence and shame** to maintain control. And in all three, the turning point came when someone spoke up. You are now more informed than most people your age about how these situations work. **That knowledge is a responsibility — to protect yourself, and to be the person a friend can turn to.**

Creative Challenge – Be a Safety Ambassador!

Activity 8 – Creative Challenge

Design an Awareness Campaign for Your School

Meera wants to turn her experience into a campaign so others don't go through the same thing. Help her design one campaign material. It must include: what grooming is, one warning sign, and one safe action. Choose Option A or Option B.

Option A: Awareness Poster

What is Grooming? (Draw/write)	One Red Flag (illustrate)
Safe Action to Take	Your slogan for HP students

Option B: Instagram Story Script (3 Slides)

Slide 1 = Hook (one fact that grabs attention). Slide 2 = One warning sign from this chapter. Slide 3 = One safe action. Max 15 words + emoji per slide.

Slide 1 (Hook):

Slide 2 (Warning sign):

Slide 3 (Safe action):

Epilogue – One Month Later

<p>Meera</p> <p>"I almost didn't tell anyone. I'm so glad I did. I'm speaking at our school's safety assembly now."</p>	<p>Aryan</p> <p>"Ch.5 = protect each other. The only thing a groomer fears is someone speaking up."</p>	<p>Priya</p> <p>"Meera's case made me audit every follow request I'd accepted. I found two accounts I'd never verified."</p>	<p>Kavya</p> <p>"She showed me the messages because she trusted me. That trust saved her. Be someone your friends can trust."</p>	<p>Naman</p> <p>"Staying silent protects the groomer. Speaking up protects everyone else. Simple choice."</p>
--	--	---	--	--

Key Takeaways

<p>Grooming Is a Process, Not One Event</p> <p>It builds trust slowly and deliberately. Knowing the 5 stages means you can spot it early — before it escalates.</p>	<p>Secrecy Is the Biggest Red Flag</p> <p>Any online relationship that requires you to hide it from parents or trusted adults is a warning sign — always.</p>
<p>It Is Never the Victim's Fault</p> <p>Groomers are skilled and deliberate. The shame belongs to them — never to the person they targeted.</p>	<p>Stop · Screenshot · Report</p> <p>Do not reply. Do not pay. Preserve evidence, block, tell a trusted adult, and report to 1098 or cybercrime.gov.in.</p>

Aryan, Priya, Naman, Kavya & Meera's Golden Rule

"A groomer's greatest weapon is your silence. Take it away. Tell someone you trust — because speaking up is not weakness. It is the bravest, most powerful thing you can do."

<p> Ch.1 Protect Your Account</p>	<p> Ch.2 Protect Your Data</p>	<p> Ch.3 Protect Your Reputation</p>	<p> Ch.4 Protect Each Other</p>	<p> Ch.5 Protect Your Trust</p>
---------------------------------------	------------------------------------	--	-------------------------------------	-------------------------------------