Cyber Safety for Students and Families

Everyday digital safety for students, parents and elders - including online bullying and gaming risks.

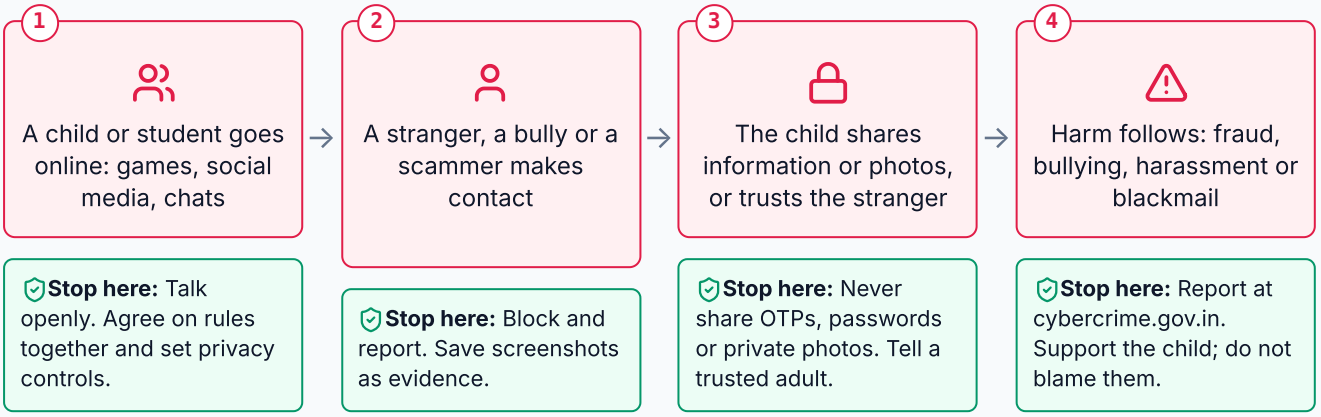
Lost money in an online fraud? Call 1930 right away and report at cybercrime.gov.in.

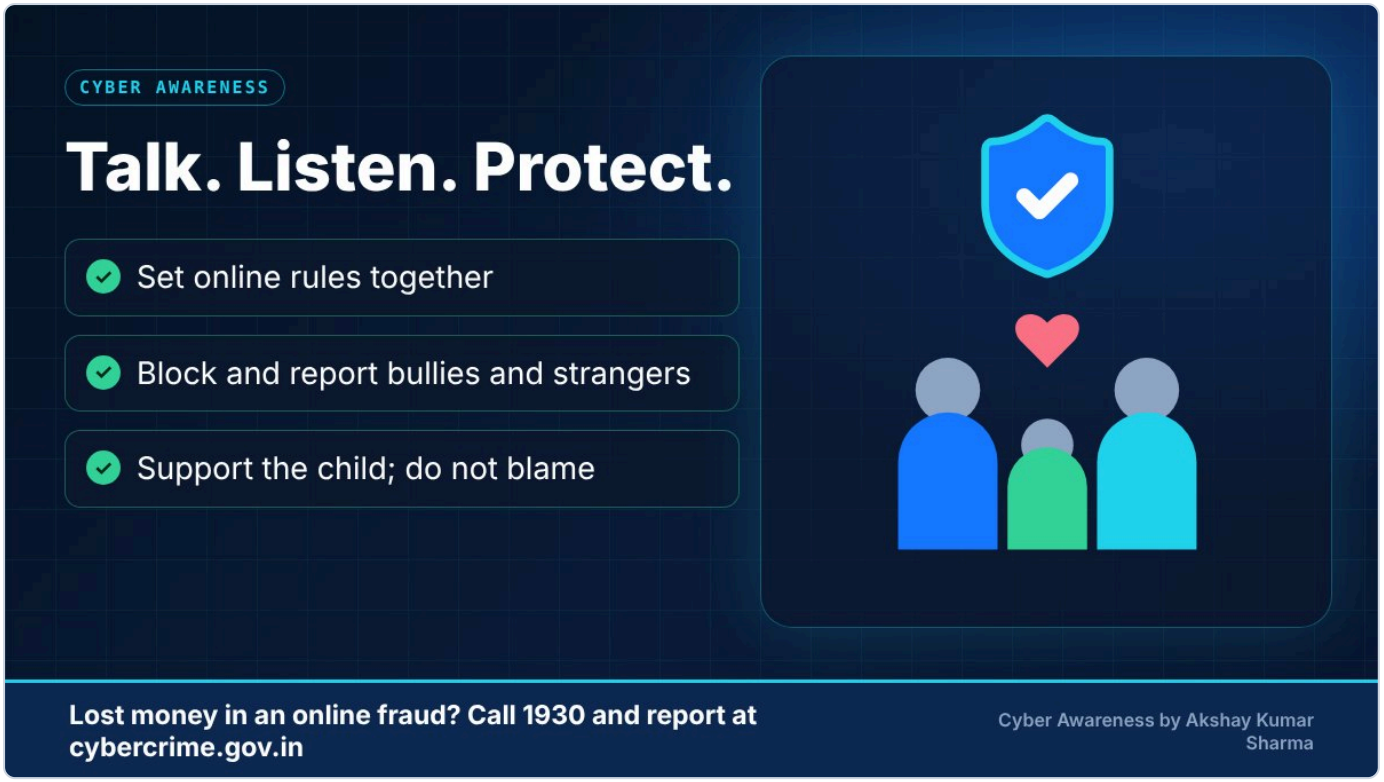
What it is

Students and families are online for learning, gaming, payments and social life. Risks include online bullying, scams promising scholarships or part-time jobs, unsafe contact from strangers, oversharing and weak account security. Open conversation at home is the strongest protection.

How it works - and where you can stop it

Red boxes show what the attacker does. Green boxes show where you can break the chain.





Common warning signs

- ⚠ A child or student becomes secretive, anxious or avoids devices after messages.
- ⚠ Contact from a stranger who asks for photos, personal details or to move to another app.
- ⚠ 'Scholarship', 'free gift' or 'job' offers that ask for fees or bank details.
- ⚠ Gaming or in-app purchases made without the family's knowledge.
- ⚠ Elders receiving calls about prizes, KYC or relatives in trouble.

Practical prevention tips

- Talk openly and make it clear that anyone can come to you without fear of blame if something feels wrong.
- Use strong passwords, two-factor authentication and parental or privacy controls that suit the child's age.
- Teach the basics: do not share OTPs, do not click unknown links, do not meet online contacts alone.
- Keep devices and apps updated, and restrict payment methods on children's accounts.
- Help elders set up payment alerts and agree to check with the family before any unusual payment.

Risky habit vs safe habit

RISKY	SAFE
✕ Scold a child for reporting a problem	✓ Stay calm, listen and support
✕ Share passwords with friends	✓ Share them only with parents or guardians
✕ Chat with strangers in online games	✓ Play with friends you know in real life
✕ Hide cyberbullying out of fear or shame	✓ Save the evidence, block and report

What to do if it happens

1. Stay calm and support the person. Do not blame them.
2. Keep screenshots and messages as evidence, then block and report the account on the platform.
3. Report serious harassment or fraud at cybercrime.gov.in and call 1930 for financial fraud.
4. Involve the school or college if the issue involves classmates.

Official reporting resources

- National Cyber Crime Reporting Portal (cybercrime.gov.in) - https://cybercrime.gov.in/
- Cyber crime helpline 1930 (for financial cyber fraud) - 1930
- CERT-In (Indian Computer Emergency Response Team) - https://www.cert-in.org.in/

Never share your banking password, OTP, UPI PIN, card CVV or full card number with anyone - not even someone claiming to be from your bank, police or a government office. This website will never ask for them.

This website is an educational resource. It is not an official government reporting portal or an emergency response service. If you are a victim of cyber fraud, report it through the official channels listed on each page.
Akshay Kumar Sharma - https://www.youtube.com/@cybersecwithakshay