WHAT CAN ONE DO IF THEY ARE A VICTIM OF CYBER GROOMING?

01 INFORM
Inform parents or elders immediately. Inform Teacher or Head of the institution if an incident occurs in school.

02 BLOCK
Block the groomer or attacker if the groomer is using a social media platform.

03 COLLECT
One must collect and save messages, pictures or videos sent by the groomer and can be used as evidence to take legal action against the groomer.

04 BEWARE
Elders/parents must be made aware so they can contact the local police station to lodge a complaint against the groomer.

HELPLINE FOR REPORTING CYBER CRIME

100
National Police Helpline Number

cybercrime.gov.in
National Cyber Crime Reporting Portal

MHA Helpline - 155260
For Delhi & Rajasthan (24*7) & For Chhattisgarh, Uttarakhand, Uttar Pradesh & Madhya Pradesh
(10:00 a.m to 6:00 pm)
COMMON THREATS IN CYBER SAFETY

PHISHING
Phishing is a type of social engineering attack often used to steal data, including login credentials and credit card numbers. Phishing occurs when attackers/scammers masquerade as a trusted entity and send text, email, or pop-up messages to get people to share their personal and financial information.

CYBER BULLYING
Cyberbullying is bullying with the use of digital technologies. It is a form of harassment or bullying inflicted through the use of electronic or communication devices such as computer, mobile phone, laptop, etc. It is a punishable offence under the Information Technology Act, 2000 and the Indian Penal Code. It also involves posting pictures or videos aimed at harassing another person.

CYBER GROOMING
Sometimes strangers, or even people who are known, build an emotional connection with children and young people online or face-to-face to gain their trust for the purposes of sexual abuse or exploitation. Many children and young people begin to feel that a special friendship or relationship is developing and do not understand that they are being groomed.

GAMING
Games can offer children a way to escape from the real world and immerse themselves in a virtual world. Increasingly, children play games on mobile phones, consoles, laptops, computers, portable gaming devices and social media. While playing you could interact with other gamers through a microphone or a webcam. Cybercriminals can find a way to victimize children through befriending them online, cyberbullying or sharing inappropriate content.

HELPLINE FOR REPORTING CYBER CRIME

100
National Police Helpline Number
cybercrime.gov.in
National Cyber Crime Reporting Portal

MHA Helpline - 155260
For Delhi & Rajasthan (24*7) & For Chhattisgarh, Uttarakhand, Uttar Pradesh & Madhya Pradesh (10:00 a.m to 6:00 pm)
‘DO’S AND DON’TS’ FOR ENSURING BULLYING-FREE CYBER SPACE

DO’S
1. Create a strong password according to password guidelines, and frequently change passwords to prevent misuse.
2. Read the privacy settings very carefully on social networking sites.
3. Communicate only with known people.
4. Be careful while posting photographs, videos and any sensitive information on websites as they leave digital footprints which stay online forever.
5. Ensure that only authorized personnel access computer systems and labs.
6. Report immediately to the support team of the networking site if you suspect that your account has been hacked or stolen.
7. Invest in a strong network security system.
8. Use only verified open-source or licensed software and operating systems.
9. Set up your computer for automatic antivirus software and operating system updates.

DON’TS
1. Don’t reveal your password to anyone other than your parent or guardian.
2. Don’t reveal personal information like age, address, phone number, school name etc. as this can lead to identity theft.
3. Don’t post anything which hurts others’ feelings.
4. Don’t post your friends’ information on networking sites, which can put them at risk.
5. Don’t forward anything that you read on social media without verifying it from a trusted source.
6. Don’t leave your account unattended after login, log out when you are not using it.
7. Don’t create fake profiles for yourself on any social networking site.
8. Don’t use personal devices such as personal USBs or hard drives on public networks or computers.
9. Don’t open links and attachment on social networking sites and block file extensions such as .bat, .cmd, .exe, .pif by filtering software.

HELPLINE FOR REPORTING CYBER CRIME

100
National Police Helpline Number
cybercrime.gov.in
National Cyber Crime Reporting Portal

MHA Helpline - 155260
For Delhi & Rajasthan (24*7) & For Chhattisgarh, Uttarakhand, Uttar Pradesh & Madhya Pradesh (10:00 a.m to 6:00 pm)

HOW TO PREVENT AND COUNTER CYBERBULLYING?

**Do not respond**
If someone is bullying you online, DO NOT respond or retaliate by doing the same thing. Responding or retaliating may make matters worse or even get you into trouble.

**Collect as much information as possible**
Take a screenshot of anything that you think could be cyber bullying and keep a record of it.

**Block and report**
If someone bothers you, make sure you block the offender and report on the social media platform immediately. This feature is available on most online platforms.

**Talk about it**
Inform trusted adults like your parents and teachers about the bullying incident. Seek help. Do not feel that you are alone and never keep it to yourself.

**Be private**
Keep your social media privacy settings high and do not connect with anybody you do not know offline.

**Be aware**
Remain updated with all the preventive and security measures in the cyber world.

---

**HELLINE FOR REPORTING CYBER CRIME**

**100**
National Police Helpline Number
cybercrime.gov.in
National Cyber Crime Reporting Portal

**MHA Helpline - 155260**
For Delhi & Rajasthan (24*7) & For Chhattisgarh, Uttarakhand, Uttar Pradesh & Madhya Pradesh (10:00 a.m to 6:00 pm)

SOURCE: NCERT (2020); Safe Online Learning in Times of Covid-19
HOW CAN ONE PROTECT POTENTIAL FROM RISKS ASSOCIATED WITH ONLINE GAMING

01 Do not share personal information like name, D.O.B, address and phone number with players while playing online games. One doesn’t know or is aware as to who the players are and what are their intention? One may end up sharing their information with scammers or cyber bullies.

02 Never share your or parents credit card/debit card details with anyone when they are playing online games. Some cyber criminals befriend children by helping them winning games or sharing points.

03 Never install games downloaded from free online gaming websites that are not reputed. Never download games by clicking on links received on mail or text message or through a pop-up. One may end up downloading viruses and malware which can compromise the security of their computer’s or smartphone.

04 Always install a good anti-virus software on one’s computer, smartphone, or handheld devices. Regularly update the anti-virus and other applications.

05 Never share passwords with anyone. One should use a complex password for their online gaming account and other online accounts. It is a good practice to change passwords at regular interval.

06 Never use voice chat or webcam while playing online games. This may share one’s identity with other players and attract cyber bullies and other cyber criminals.

07 Never meet in person with someone from one’s online gaming world.

08 If anyone faces any challenge in online gaming world, one must immediately inform their parents or elders so that they can gain immediate support and guidance.

HELPLINE FOR REPORTING CYBER CRIME

100
National Police Helpline Number
cybercrime.gov.in
National Cyber Crime Reporting Portal

MHA Helpline - 155260
For Delhi & Rajasthan (24*7) & For Chhattisgarh, Uttar Pradesh & Madhya Pradesh (10:00 a.m to 6:00 pm)

SAFETY ON SOCIAL MEDIA

Schools shall not allow use of social media platforms in schools by students, teachers or anyone engaged in school

**Setting Profile to Private**
One must think carefully about what one posts online and who should be its audience. Children should be educated to consider setting their profile settings to 'friends/followers' only.

**Remember anything you post can be shared**
Children must be educated that even with strong privacy settings in place, it is important to know that whatever one posts online is never private and can be shared. It is therefore important that one must always think before posting.

**Recognize the fakes**
Children must be educated that not everyone on social media will be who they say they are. There can be young people and adults who pretend to be someone else and could cause harm. For example: They may want to trick you into sharing private or personal information that they could use against you. It’s important that one should never meet up with someone you don’t know, and that you always let an adult know where you are going and who you are meeting.

**Protect your identity**
Children must be educated that their phone number, address, bank details and any information that may hint at their passwords should never be shared.

**HELPLINE FOR REPORTING CYBER CRIME**

<table>
<thead>
<tr>
<th>100 National Police Helpline Number</th>
<th>MHA Helpline - 155260</th>
</tr>
</thead>
<tbody>
<tr>
<td>cybercrime.gov.in</td>
<td>For Delhi &amp; Rajasthan (24*7) &amp; For Chhattisgarh, Uttarakhand, Uttar Pradesh &amp; Madhya Pradesh (10:00 a.m to 6:00 pm)</td>
</tr>
</tbody>
</table>