सत्यमेव जयते

A Handbook for Adolescents/ Students on Cyber Safety

Ministry of Home Affairs
Government of India

Cyber Grooming

Cyber Grooming is growing as one of the major cyber threats faced by children and teenagers. It is a practice where someone builds an emotional bond with children through social media or messaging platforms with an objective of gaining their trust for sexually abusing or exploiting them.

The cyber groomers can use gaming websites, social media, email, chat rooms, instant messaging, etc. by creating a fake account and pretending to be a child or having same interests as of the child.

Do you know that many of us don't even realize that someone is grooming us online? Online groomer can be a known person, a relative or even an unknown person whom we met online on social media platform, a chat room or gaming portal, etc.

Initially, the cyber groomer can give you compliments, gifts, modelling job offer and later they can start sending obscene messages, photographs or videos and will ask you to share your sexually explicit images or videos with them.

The online groomer mostly target teenagers as in adolescence they face immense biological, personal and social changes. The impulsive and curious nature of adolescents encourages them to engage in online activities which makes them vulnerable to online grooming.

The cyber grooming has deep impact on a child's physical, emotional as well as psychological well-being. It can not only impact their academic performance but also their daily life to a great extent. The devastating effects of online grooming can sometimes be long-term and can even haunt the victim in their adulthood

Concerned about cyber grooming? Don't worry... with awareness and precautions you can use internet and mobile technology without any fear. You need to be careful and follow safeguards to protect yourself and your friends against cyber grooming.

Let's discuss how you can protect yourself from becoming a victim of cyber grooming

- Don't accept friend request from unknown people on social media platforms. Cyber groomer can even create a fake account to befriend victims.
- Don't share your personal information like date of birth, address, phone number and school name on social media or other online platforms. You can go to privacy settings on social media platforms to select who can access your posts online. Try to restrict access of your profile to your friends only.
- Be cautious when your chat partner gives you many compliments regarding your appearance in just a short span of your acquaintance.
- Avoid talking to people who asks you questions related to your physical or sexual experiences. You can tell the person to stop asking you such questions as you feel uncomfortable. If they continue to do the same, immediately inform your parents.

- Do not talk to people who ask you to share your sexually explicit photographs or videos. If you share your sexually explicit photos or videos with someone, the person can share those photos with others or post them on social media. They can also blackmail you.
- Never turn on your webcam while your chat partner does not connects to the webcam
- Talk to your elders or parents, if your chat partner suggests to keep your conversation with them a secret.
- Do not go to meet a person whom you met online alone. Always take a friend or an elder person with you.
- Never install unwanted Software and Apps like dating App, online games, etc. from unknown sources. You should be very careful while chatting in the chat rooms. Never share personal details in the chat room and limit your identity.

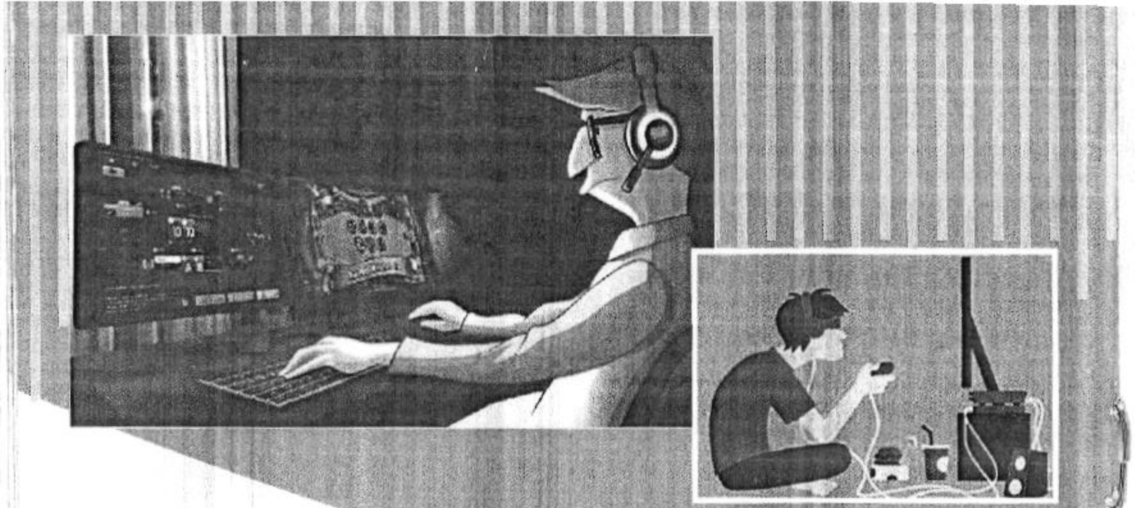
What can you do if you are a victim of cyber grooming?

If you feel that you are a victim of cyber grooming, please inform your elders so that they can intervene and support you. Following suggestions can be helpful in managing the situation.

- **Inform your parents / elders immediately:** If someone online is making you uncomfortable, you must inform your parents / elders immediately. Don't feel that your parents will restrict your online activity or ask you not to use your computer / smart phone. It is important to inform them so that they can support and guide you. Narrate the entire issue clearly to your parents/elders.

- **Block the Groomer:** If groomer is using social media platforms to groom you, you can block him/her. All the social media apps or services have the option to block a user.
- **Collect and Save messages:** Save messages, pictures or videos shared with you by the groomer. Such messages, pictures or videos can be used as an evidence to take a legal action against them.
- Your parents/elders can contact local police station to lodge a complaint against the groomer.

Do you know that producing, publishing and transmitting sexually explicit material or Child Sexual Abuse Material (CSAM) is electronic form is a punishable offense under The Information Technology Act 2000 of India?



ONLINE GAMING

Surprised how online gaming is related to cyber security? Let me tell you that more and more children and young people are gaming online and the number is going to increase many fold in future. Where ever there are lot of users on internet, cybercriminals find their way to victimize them. This can be in way of cheating, cyber bullying, sharing inappropriate content, etc.

Gaming is another area which has been transformed with the advent of information technology. More and more children are joining the online gaming community. Easy access and variety of platforms that can be used for playing online games have helped in increasing online gaming in India. Children can play online games on mobiles, consoles, computers, portable gaming devices and social networks. The gaming consoles operate like a computer where you need to create your account, login, put a headset, use web cam or other devices. You not only play games with crores of users online but also talk to them, share your views, become friends, join groups, teams, etc. There are crores of players playing online games at any given point in time. While online games can be fun, they also bring associated risks.

Do you know that you may end-up downloading spam, viruses, malicious software along with the online games that can adversely impact your computer or mobile phone or gaming console? It is important to download games from reputed sites. Never download/ install pirated games and software.

It is a matter of concern that outdoor activities and physical games are missed out on by our computer and smart phone-loving children. It is advisable to include outdoor games in addition to online games that helps you in your overall physical, mental and social development.

Given the range of online games available and ease of playing with crores of players online from across the globe, online gaming can be a fun way for you to connect with others, but it is indeed important for you to understand the associated risks and know how to handle certain situations. Enjoy the online gaming experience and have great fun, but make sure that you play it safe!!!

Do you know what are the risks associated with online gaming?

- ☞ There are many aggressive players online who may bully you. Some players play simply to bully or harass others. They may use inappropriate language or cheat others. It is important for you to be careful.
- ☞ Many adults and cyber criminals also play online games and pretend to be a child. They may try to befriend you by giving tips about the games, sharing points with you and trying to win your trust. They may use this opportunity to run a scam by

getting personal information or motivating you for a one-to-one meeting.

- There are many free online gaming websites. Moreover, you may receive links over emails or text messages to download an interesting online game. Some of the games ask lot of personal information about the player before creating an account. This may compromise your personal information like your name, age, mobile number, etc., which can be misused. You may end-up downloading viruses or malwares along with free online games downloaded from unsecure sites which can infect your computer, smart phone or other gaming devices.
- In many online games you are asked to buy points/coins, etc., which can be used to improve performance or give you advantage in terms of time or resources. You are asked to share credit card details for the payment. Of course you ask your parents to help you with the purchase. However, some infected online games can capture your credit card details and misuse it.

Concerned about online gaming? Don't worry... with awareness and precautions you can play online games safely. You need to be careful and follow safeguards to protect yourself and your friends from potential risks associated with online gaming.

Let's discuss how you can protect yourself

- Don't share your personal information like name, date of birth, address, and phone number with players while playing

online games. You don't know who the players are and what is their intention? You may end-up sharing your information with scammers or cyber bullies.
- Never share your or your parent's credit card/debit card details with anyone when you are playing online games. Some cyber criminals befriend children by helping them with winning games or sharing points. They may win your trust and later ask for your help to buy coins/points, etc. They may ask credit or debit card details. Never share such details with anyone.
- 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 popup. You may end-up downloading viruses and malwares which can compromise security of your computer or smart phone.
- Always install a good antivirus software on your computer, smartphone or other handheld devices. Regularly update the antivirus and other applications.
- Never share your passwords with anyone. You should use a complex password for your online gaming account and other online accounts. It is a good practice to change your password on regular interval.
- Never use voice chat or web cam while playing online games. This may share your identity with other players and attract cyber bullies and other cyber criminals.
- Never meet in person with someone from your online gaming world. In real life they may be very different. Cyber criminals

duplicate SIM. They obtain the duplicate SIM from service provide and use it to transact online using your mobile number and banking app.

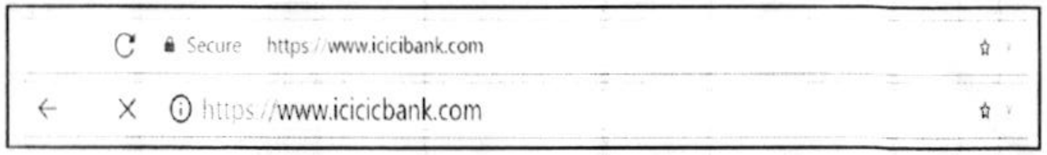
Do you know that bank would bear the loss of banking frauds only if negligence or security laps is found at bank's end?

Total 1785 cases have been reported related to credit/debit card and Internet banking fraud in the year 2017 alone. This amounted to a total loss of R.s 71.48 crores.

Concerned about online transaction frauds? Don't worry...with awareness and precautions you can safeguard yourself against online transaction frauds. Please remember if you don't share your bank and card details like card number, PIN, CVV, expiry date,bank account password, etc., with anyone, you may be able to protect yourself against online transaction frauds. You need to be careful and follow safeguards to protect yourself and your friends against such frauds.

Let's discuss how you can protect yourself from becoming a victim of online transaction frauds. Don't forget to share these suggestions with your family and friends.

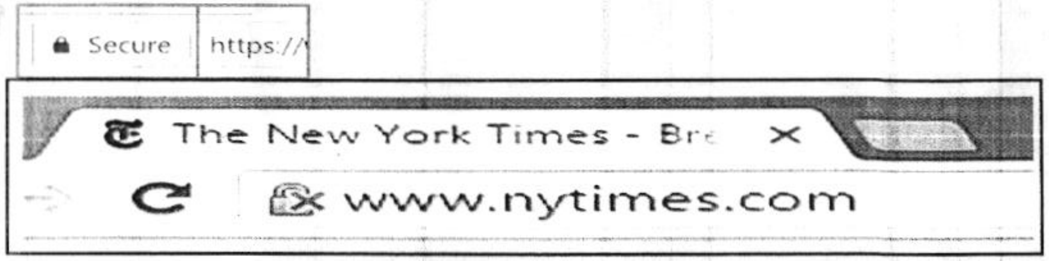
- Never share your bank and card details such as online account password, card number, CVV, expiry date, PIN, OTP, etc., with anyone. By sharing these details you will compromise your account which can lead to illegal online financial transactions.
- Make it a habit to regularly update your online password of your bank account and PIN of your Debit/Credit cards.
- Always make it a habit to type bank website yourself when trying to login to your bank account. You must not click on a link of bank website appearing on an email, text message or a popup. This may be a fake link and may take you to a fake site. Once you login to your bank account from a fake site, your sensitive details like account number and password may be stolen.



Secure https://www.icicibank.com

https://www.icicibank.com

- Check for the bank's security certificate details and various signs such as green address line, lock sign on the address bar and HTTPS to confirm you are visiting a secure bank website



Secure https://

The New York Times - Br

www.nytimes.com

- Always check the website URL starts with HTTPS. The website URL with HTTPS encrypts your data in the website and protects it from any kind of tampering. Do not share your confidential information such as online account password, card number, CVV, expiry date, PIN, OTP, etc. on the website which doesn't start with HTTPS.
- It is equally important to protect your mobile phone as your mobile number is linked with your bank account. Always use a strong password to open your mobile phone and install a good antivirus software. If you receive a call from mobile service provider informing you that your number will be deactivated if you don't update it or any other such message, please be

cautious. Disconnect the phone and call customer care number of your mobile service provider to check if the call was genuine.

- Never install pirated software on your mobile or computer. It is not only illegal but may also compromise security of your devices. Always install a good antivirus on your computer and mobile phone. It is important to keep your computer software and anti-virus up-to-date.
- Avoid making online transactions using a public Wi-Fi or a computer in a cyber café. Computers in the cyber café may not have updated antivirus or may be infected with malware which may compromise your bank details and other sensitive information such as card number, expiry date, CVV, etc.
- Make it a habit to review the monthly statements of your bank account and credit cards. Check if there is any unrecognized transaction.
- If you find that your bank account or card details are compromised/stolen by someone or your debit or credit card is lost, call the bank immediately and block your card/account immediately. If unauthorized transactions have taken place, you must lodge a formal complaint at your nearest police station.

Safeguards for your social networking profiles

Social networking sites such as Facebook,Twitter, Instagram, Snapchat, etc., are extensively used by all of us. We love sharing an update or a selfie or pictures with our friends and relatives. We love receiving likes and comments on our posts/pictures and updates. While social networking sites have helped us in connecting with our friends and relatives easily, there are serious cyber threats that can impact us if we are not careful.

How it works?

Cyber criminals and cyber bullies can use social networking platforms to harm us. Let us learn about common cyber threats related to social networking sites which can impact anyone of us.

- Cyber criminal can create your fake account on social media and use it to share negative things and inappropriate content to harm your image or for other illegal purposes. This is a very real threat and can impact anyone. It is easy to create a social media account using any email id. These days our pictures, email id, date of birth and other details are easily available online. Cyber criminals can use these details to create our fake account.

- Cyber bullying is very common on social media platforms. Cyber bullies can use social media to send rude or hurtful messages to demean or hurt you.
- Online frauds can be triggered through links shared on social networking sites. Cyber criminals share a post with a malicious link or a malware. If you click on the link, your computer or mobile can be infected or compromised.

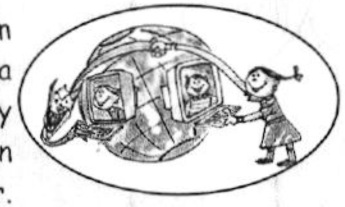
Concerned about cyber threats on social networking platforms? Don't worry... with awareness and precautions you can safeguard yourself and use social networking sites safely. You need to be careful and follow safeguards to protect yourself and your friends against such frauds.

Let's discuss how you can protect yourself and your social media accounts. Don't forget to share these suggestions with your family and friends.

- First important step is to safeguard your own social networking account so that it is not hacked or compromised. For this you must use a complex password and change it periodically.

Do you know that most of the social media sites and email service providers give you an option of two factor authentication to login in to your account? You can go to settings and activate two factor authentication. This means you will need to type your password and One Time Password (OTP) received on your mobile to login to your account. It is a good safety feature and should be used for all your accounts.

- Never share password of your social media account with anyone. Sharing password may compromise your account.
- Whatever you post on social networking sites can be visible to everyone unless you restrict the access of your posts to your friends/followers. You must change the privacy settings of your social media account and ensure that your updates/posts, etc. are visible to your friends/followers only.



- Avoid accepting friend request from unknown people. Before accepting a friend request try to see how many other people are following or are in friend's list of the requestor. Cybercriminals can create fake account of your known person so be careful.
- Whatever you post on social media generally remains there. Be careful before posting anything on social media. Think if the information can be shared with everyone. Never share your personal details such as address, phone number, date of birth, etc. on social media sites.
- If you are using computer of your friend or a computer in a cyber café to access your social media accounts, make sure you don't click yes on "remember password popup" which generally comes when you login from a new computer. You must never allow any computer to remember your password (this means password will not be required to login to your account on that system). Always remember to sign off from your account after using it.
- If you are accessing social media accounts on your mobile phone,remember to keep a strong password to access your phone.
- If your social media account is hacked/compromised, send an alert email or message to all your contacts. Immediately ask your social media service provider to temporarily block your account. Try to retrieve your password and change your password immediately.
- If you notice that your fake account has been created, you can immediately inform social media service provider so that the account can be blocked. If someone is bullying you, posting inappropriate comments or images or creating your fake account to damage your image, inform your parents or elders

immediately so that they can support and guide you. With support from your parents, you can also register a complaint at your nearest police station.

- Never install unwanted software and apps from unknown sources. Never click on links or files received from unknown person on social media. This may be an attempt to infect your computer with a malware.
- Fake news or Hoax messages spread like wildfire on social media. It may create law and order problem and may end-up causing loss of life in few cases. Before forwarding or sharing any message on social media or messaging app, check it on other sources also to confirm its authenticity.
- Never download or upload copyrighted content such aspoems, essays, videos, music, images, composition of songs, music, software, etc. without the author's permission. The act of downloading and uploading copyrighted work of others is an offence.

Hope you enjoyed reading this handbook. These suggestions should help you in protecting yourself from cybercrimes. As you know cybercriminals frequently devise new ways to cheat people. It is important to remain up to date with new threats and ways to protect ourselves.

Few suggestions from your CyberDost

- Read more about cybersecurity, emerging new threats and ways to safeguard against cybercrimes.
- Be a good cyber citizen. Use precautions yourself and educate your friends and family about cyber security
- You can follow us on twitter handle @ Cyber Dost for regular updates on safe cyber practices.
- We request you to please share your feedback with us on dircis2-mha@nic.in or pmuiec.cis-mha@nic.in