CYBER SAFETY FOR ADOLESCENTS

[1]Anitha.P, [2] Prema Balusamy
[1]Research Scholar, [2]Assistant professor
[1]Faculty of Nursing,
[1]Bareilly International University, Bareilly, India.

Abstract : Cyber safety is the safe and accountable use of data and communication technology. It is regarding keeping personal data safe, secure and self-protection from cybercrimes. Adolescents are exposed to various crimes like cyber bullying, cyber grooming, online gaming fraud, email fraud and so on. Adolescents should aware about how the cybercrime happens, occurs through, various forms, how to protect them self and how to report in case of you are victim.

Keywords: **Cyber safety, cyber bullying, cyber grooming, online gaming fraud, email fraud, Adolescents**

Introduction

Cyber is a prefix derived from the word informatics and has the general meaning of through the use of a computer which is also called as cyberspace. [1] The cyber space connects millions of online users across the world and increasing use of cyber space, cybercrimes also increased. Adolescents are most commonly exposed cybercrimes like cyber bullying, cyber grooming, online gaming fraud, email fraud and how to report it in case of they are the victim. [2]

1. CYBER BULLYING

Cyber Bullying is that the use of the cyberspace and related technologies to hurt people during a deliberate, repeated and aggressive manner. [2]

Severe forms of Cyber Bullying

Cyber Bullying is taking place in various forms like posting, public photos, Sending inappropriate text messages, giving negative comments, Blackmailing with certain demands, Threats of violence or death, aggressive communications or actions, posting recorded photos or videos which are taken without the subject's knowledge, Sexually explicit.[3]

Cyber bully occurs through:

Personal websites, blogs, e-mail, texting, social networking sites, chat rooms, message boards, instant electronic messaging, photographs. [4]

Cyber bullying may relate to

1. abuse (or)
2. harassment by teasing or insulting a victim's

- body shape
- intellect
- family background
- dress sense
- mother tongue
- place of origin
- attitude
- race
- caste
- name calling

How to Prevent It

- **Never** - share your passwords, personal photos, or personal knowledge online, not even with friends. Try and limit your identity.

- **Privacy settings** - on social media to select those who can access your posts online. Restrict access of your profile only to your friends.
- **Think** -before you post. When you're sad, angry or depressed wait to post or respond.
- **Never** - publicly post anything which wouldn't be comfortable with people who know you like your parents and friends.
- **Never** install unwanted Apps and software like dating apps, online games, etc. from unknown sources.[5]

What to do if you're being cyberbullied

- **Tell** your parents or another trusted adult.
- **Don't respond**—they might use it against you
- **Block** the person who harassed you and change your privacy settings
- **Save everything** – emails, messages, posts, screenshots etc. save the proofs don't delete it.
- **Report- to** Social media sites where you have ways of reporting harassing content with proofs.

If you are one of the observer

If you see someone being bullied online:

- **Don't participate**. Don't entertain, don't "like" or share any post that are bullying someone.
- **Report it**. Still you can report it though the content is not targeting you. [2]

2. CYBER GROOMING

Cyber grooming is growing together of the main cyber threats faced by children and teenagers. It is an act of where someone builds an emotional bond with children through social media with an aim of gaining their trust for sexually abusing or exploiting them. In the first place the cyber groomer can get a sure through giving you compliments, blessings, and work offer and later they can begin sending revolting messages, photos or recordings and will request that you share your explicitly express pictures or recordings with them. [6]

Signs of grooming

Online groomers are really good in the beginning, which means it can be difficult to get if someone is really an online friend, or if they're trying to get you to send them sexual images or videos.

Some of the following they can do:

- Send you lots of messages
- Ask you to keep your conversations secret
- Try to find out more regarding your privacy
- Start sending you sexual messages
- Get to know about your personal information for try to meet you
- Blackmail you.[2]

How can you protect yourself from cyber grooming?

- Never give out your real name

- Don't accept friend request from the people who you don't know on social media.
- Don't share your personal information like address, date of birth, mobile number and school name on social media or any other online platforms. You can do settings in privacy on social media platforms to choose who can access your posts online.
- Be cautious when your chat partner gives you many compliments regarding your appearance in just a short span of your contact.
- Avoid talking to people who asks you questions about physical or sexual experiences. You can warn the person to stop asking you such type of questions and immediately inform your parents
- Never talk to people who ask you to share your sexually explicit photographs or videos. Buy sharing your photos, the person can share to others and also blackmail you.
- Inform to your elders or parents, if the person wants to maintain a secret conversation with you.
- Do not try to meet a person to whom you met online alone. [6]

What are you able to do if you're a victim of cyber grooming?

- Inform your parents / elders immediately:

- Block the Groomer
- Collect and Save messages.
- Your parents or elders shall contact local police station to lodge a complaint against the groomer.[7]

3. ONLINE GAMING

Gaming is another area which has been changed with the coming of data innovation. An ever increasing number of children are joining the internet gaming network. Children can play web based recreations on mobiles, PCs, compact gaming gadgets and social networks. You not just play amusements with crores of clients on the web yet additionally converse with them, share your perspectives, become companions, join gatherings, groups, and so forth. While web based amusements can be fun which additionally bring related dangers.[2]

Risks of online games

1. Many violent online players who may bully you. Some of them play intentionally to bully others.
2. Many cybercriminals pretend like they are children and try befriending with others. After gaining confident with others try to get personal information for grooming.
3. There are many free internet gaming sites. Additionally you may get links and emails to download and get personal information like your name, age, mobile number, and so on, which can be abused. You may finish up downloading infections or malwares which may infect your computers
4. In numerous internet games you're requested to purchase points /coins, and so forth and you are approached to share credit card details for the payments. Moreover some infected online games can save your credit card details and do cybercrimes.[8]

How you can protect yourself while online gaming

- Link based scams and phishing is common in game chat so when you are receiving from the stranger we have careful and don't open it.
- Never share your account information if you get an email and say you won the prize ad asked you to enter the user name and password. Always use two factor authentications to protect your account.
- Don't use personally identifiable information. Never use this because its leads to identity theft. Personally identifiable information are, Full name, Postal address, Name and address of school, mailing address and phone number, Passwords, Credit card number, Social security number, work place, Photo's

  These are the examples you can share

  Age, sex, number of siblings, favorite color, favorite food, the name of your pet, Your opinion about some common issues. [2,8]

- Make a habit of change your password regularly.
- Never download games by the links which you have received by mail or text message or through a popup. You may wind up downloading infections and malwares which can bargain security of your PC or mobile.
- Never meet face to face with somebody from your online gaming world.
- If you face any problem in internet gaming world, quickly inform to your parents or to adult to whom you trust. [6]
- Create a habit of playing outside recreations. You will appreciate open air exercises and can make genuine great companions

4. EMAIL FRAUD

Email fraud is normal and most economical technique utilized by cyber criminals to bargain other email represents individual increase or to make harm person.

How it happens

- A cybercriminal settling down anyplace in the world can send you an email which may like from a fake account. you may get to know the fake account by seeing the mail for example spelling might be slightly changed - customer support @ gamingpportal.com here you can see the pportal spelling is wrong. These messages contain joins which would guide you to another page where you would be approached to enter passwords/certification for upgrade. Lastly you end up giving your accreditations to cybercriminal.
- Another way generally utilized by cybercriminal is sending an email with an attached file (word or excel file) which may contain malware (hazardous program that can affect your PC). The title shows that tips to

win the game or to get free coins. If you install such documents it may catch your id and password from your computer and send them to others.

- Do such messages they ask for the personal information like bank details for sending the amount or they may ask the processing fee to send the gift or amount. Such emails are fake so better to not respond to such mails.
- Email hacking is one of the way the cyber criminals follows to get you mail id and password through malware. Once its hacked it may direct them to other social media accounts, bank accounts etc. Moreover they send mail to others those who are in your address book and seek for financial help or for cyber grooming.[2]

How you can protect yourself

- Before opening the email first see for the sender name
- don't reply to SPAM
- change your password periodically
- Create a strong and complex password so that criminals unable to hack your email. Password always should be difficult to guess so which has combination of words and numbers
- Always use two factor authentications for login. It is always allow you to login through password and OTP which you receive into your registered mobile number.it will help you to keep your account safe.
- Never share password to anyone.
- Don't click online or attachment which you have received from unknown sender.
- If you use others computer for email access make it sure that to sign off after the use and never click the option of "remember password popup" .change the password once you used the public computer.
- If your email is hacked immediately block your email id through your service provider by help page. Take action to change your password.
- Never click on links or files received from person who doesn't know on your email or over message. This will try to infect your computer or phone with malware.
- If you receive an email about winning a lottery or prize, please don't respond to it and share your personal information like name, address, bank account details, etc.
- develop a habit of changing the passwords at regular intervals
- Don't reply to the strangers
- Inform to parents in case of mail message make you to feel uncomfortable.[6]

How to report the cybercrime

Ministry of Home Affairs, Government of India has set up The National Cybercrime Reporting Portal. It facilitates to report all types of cybercrimes with special focus on the cybercrime against women and children. The reporting portal is https://cybercrime.gov.in.

The user need to provide the information related to the incident / complaint should be complete for the police authorities to take necessary action.it is recommended that a user uploads the evidence with the complaint which might help police authorities for prompt action. However the complaint also be reported by providing information like website address, WhatsApp number etc.

The complainant will receive a tracking number which can be used to track the progress of the compliant by clicking on check status option on the portal. There are some additional features also there like recover your user name if you forget your user name, update mobile number and can withdraw your registered case also.[10]

Conclusion

The internet has eased out our lives remarkably but at the same time, has also opened a few doors to crime.so it's our duty to keep those doors locked.so far we have seen the different crimes and ways to protect ourselves and it's our duty update our self from new threats and make aware of others too.

Reference

1. The department of science and technology. Basic research of science and technology. 2017 Jan 9.Available from: http:dst.gov.in/basic-research-cyber-security.
2. Ministry of home affairs .hand book for adolescents /students on cyber safety .2018 oct 31. Available from: https://mha.gov.in/sites/default/files/CyberSafety_English_Web_03122018.pdf

3. Cyber safety: An interactive guide to staying safe on the internet. Available from: https://www.opencolleges.edu.au/informed/cyber-safety/. [Accessed 24th April 2021].
4. The hope line *.how cyber bullying impacts students.* Available from: https://www.thehopeline.com/cyberbullying-impacts-students/.[Accessed 24th April 2021].
5. MAUCORS. Stop cyber bullying. Available from: http://maucors.govmu.org/English/Cybercrimes/Pages/Cyberbullying.aspx. [Accessed 24th April 2021].
6. Vikaspedia. Cyber Safety for Adolescents. Available from: https://vikaspedia.in/education/digital-litercy/information-security/a-handbook-for-adolescents-students-on-cyber-safety#:~:text=calling%20for%20trouble.-,Cyber%20Grooming,sexually%20abusing%20or%20exploiting%20them. [Accessed 24th April 2021].
7. TECH SPECS MART.cyber security. Available from: https://www.techspecsmart.com/what-is-cyber-grooming-how-to-avoid-cyber-grooming/.[Accessed 17th April 2021].
8. Internet matters. Online gaming- The risks. Available from: https://www.internetmatters.org/resources/online-gaming-advice/online-gaming-the-risks/#risks. [Accessed 20th April 2021].
9. Get safe online. online gaming. Available from: https://www.getsafeonline.org/protecting-yourself/online-gaming/.[Accessed 20th April 2021].
10. Ministry of home affairs. National cybercrime reporting portal. Available from: https://cybercrime.gov.in. . [Accessed 18th April 2021].