



Online Safety Awareness Guide

Safe Your Child's Digital Life

Is your child
safe online?



DR. KASHIF LAEEQ

PhD (CS), M.Phil. (CS), MCS (CS), M.Sc. (Math)
Member of IACSIT, IEEE, IEEEP, IJSER, ACM Research Group
Asst. Professor, Dept. of Computer Science
Federal Urdu University, Karachi
kashiflaeeq@yahoo.com
Ph. 03004943888

December 2020
Version 1.0

Table of Content

Contents

1	INTRODUCTION	5
1.1	MONITORING YOUR CHILD’S DIGITAL LIFE.....	5
1.2	SHOCKING FACTS ABOUT DIGITAL LIFE	6
2	BE SMART WITH ONLINE PREDATORS	7
2.1	ALWAYS HANDLE ONLINE POSTS CAREFULLY.....	7
2.2	WHAT CAN PARENTS DO ABOUT PREDATORS.....	8
2.3	WHAT CAN CHILDREN DO?	10
2.4	PUBLIC WI-FI AND ONLINE PREDATORS.....	11
3	WHY PLAYING ONLINE GAMES ISN’T ALL FUN	13
3.1	SHOCKING STORIES ABOUT ONLINE GAMES.....	13
3.1.1	<i>The Cinnamon Challenge.....</i>	<i>14</i>
3.1.2	<i>Fire Fairy</i>	<i>14</i>
3.1.3	<i>RapeLay.....</i>	<i>14</i>
3.1.4	<i>Mariam Games</i>	<i>15</i>
3.1.5	<i>The Blue Whale</i>	<i>15</i>
3.2	PARENTAL GUIDE FOR GAMING.....	16
3.3	HOW TO RECOMMEND ONLINE GAMES.....	16
4	DANGERS OF CYBERBULLYING	17
4.1	SIGNS YOUR CHILD IS BEING CYBERBULLIED.....	18
4.2	PARENTAL GUIDE FOR CYBERBULLYING.....	19
5	SOCIAL MEDIA SAFETY FOR YOUR CHILDREN.....	20
5.1	SOCIAL MEDIA FOR CHILDREN AND TEENS.....	21
5.1.1	<i>Messenger Kids.....</i>	<i>21</i>
5.1.2	<i>YouTube Kids</i>	<i>22</i>
5.1.3	<i>Google for Kids Search Engine</i>	<i>23</i>
5.1.4	<i>Kiddle for Kids.....</i>	<i>24</i>
6	HOW TO REPORT CYBER CRIMES IN PAKISTAN	25
6.1	REGISTER A COMPLAINT THROUGH FIA	26
6.2	FILE A REPORT VIA IC3	28

About the Authour

Dr. Kashif Laeeq is affiliated with the Department of Computer Science, Federal Urdu University Karachi as an Assistant Professor. He completed his Ph.D. in computer science, from National University of Computer & Emerging Sciences, FAST-NU Karachi. Apart from this, he also holds MPhil (computer science), M.Sc. (mathematics), and MCS degrees. He has been involved in teaching and research at the graduate and postgraduate level for the last 15 years. He has published more than 24 research publications in journals and conferences of



international reputation including a patient submission. He is also a co-author of a global book of the cyber-physical system. During his pedagogical journey, he has won several achievements including the HEC Indigenous PhD scholarship, two best paper award, and teacher of the year award. He is working as a technical and program committee member for different international journals and conferences and also serving as a board member of various Karachi chapters. He is also an active member of various research groups, including ACM, IJSER, IACSIT, IEEE, and IEEEEP. He also conducted many training workshops specially designed for youth to train them with the knowledge of cutting-edge technology. Some noticeable workshops are, 'technology at the frontiers of knowledge', 'how to stay protected online', 'technology can enhance your learning' and 'Social Privacy: contacting and being contacted by strangers'.

He has proved himself as the best trainer, teacher and researcher. His research interest is in cyber safety, cutting-edge learning technology, distance learning, social computing, distributed systems and virtual learning environments.

PREFACE

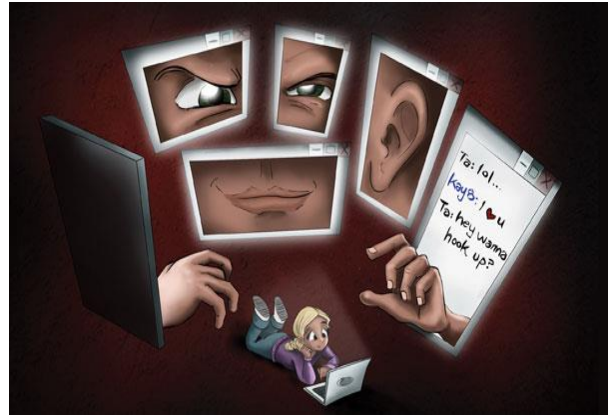
The Internet can be wonderful for your children, they can use it to complete school reports, homework, communicate with teachers and other buddies, and also play mind developing games. It is clear that many parents and teachers lack the Internet skills and awareness to properly protect their children from an extensive range of online dangers. Sadly, there are multiple cases have been reported where children die by suicide just because of Internet-related issues. There's a wide range of dangers that can affect children and teens online. This guide will uncover some shocking facts about today's Internet that you don't know before. You will also find the top online risks of the today's online world and also know how to respond to them wisely.

1 Introduction

1.1 Monitoring Your Child's Digital Life

Tell me truly you ever think what your child see, hear, and speak on the Internet, who they meet, and what they share. Before reading further just read these questions carefully, and try to answer by yourself.

1. What are the dangers of using the Internet for children?
2. What prevention children can do to avoid these dangers?
3. What parents can do to deal with these dangers?
4. If your child safety is threatened online, whom you will report?



Have you ever think about these questions, or discussed them with an expert? Researchers explain that most of the parents are too much bother about the physical life of their children, but pay no attention to their digital life. This *Online Safety Awareness Guide* will educate you in the direction to answer all these above questions. First of all, we all have to keep in mind that the frontal lobe, the impulse control and decision making part of our brains is not fully developed until our early 20s. The children and teenage group do not always understand the permanent and future consequences of today's



actions. This means when your children or their friends are dealing with unsupervised Internet, they need guidance from trusted adult such as parents and teachers. Current research says that today's youth spends more time in digital life as compared to their physical life. Parents always anxious about their

children personal belongings, schooling, career counselling but never think about their online activities, which may more dangers than any other dangerous. It looks more difficult for parents to protect their children from numerous threats on the Internet, but they should aware of what their children see and hear on the Internet, who they meet,

and what they share. Parents can save their child only when they prepare themselves about the modern knowledge of the digital world and current social media trends.

This guide is precisely designed for everyone who wants to be a better parent and safe internet user and also stay up-to-date about the latest technologies, apps and social media trends. It will raise awareness of the dangers of unsupervised Internet access for children and teenagers.

1.2 Shocking Facts about Digital Life

According to the latest research, teens spend an average of 9 hours a day online, compared to about 6 hours for those aged 8 to 12, and 50 minutes for kids between 0 to 8 years. It shows you that kids spend more time with media and technology than they do with their parents, time in school, or any other thing. This time is called Screen Time. Professor Robert Lusting, said at a conference that “kids are definitely addicted, it’s not a drug, but it might as well be. It works the same way...it has the same results.” According to WHO’s recommendation, Infants younger than 1 should never be in front of digital screens. Kids’ ages 2 to 5, the American Academy of Pediatrics said, should have no more than 1 hour each day of screen time.



Kids and teens age 8 to 18 spend an average of more than seven hours a day looking at screens. The new warning from the AHA recommends parents limit screen time for kids to a maximum of just two hours per day. For younger children, age 2 to 5, the recommended limit is one hour per day. Research has linked screen time with an increased amount of lazy behavior in children and teens. Off course, this behavior link with an increased risk of health issues, including cardiovascular disease, high cholesterol, obesity etc.

2 Be Smart with Online Predators

The Cyber Predator are people who uses the internet to exploit children and/or teens with the intention of imposing erotic, emotional, psychological, or financial abuse. They connect with children and teens through chat rooms, instant messaging, social networks, video games, and other online ways. They mostly pretend to be someone else, or lie about themselves to gain trust of their victims. A predator's goal is to trap a child into believing they care more than his or her parents or family. Mostly, they creates a false online personality that emotionally gain the trust of children.



These days' sexual and other predators often grasp children on the internet, taking advantage of their innocence, lack of adult supervision and abusing their trust. This can



end in children being trapped into dangerous personal encounters. The safety risk of cyber predators is not only the mental and emotional abuse they intend to inflict on their victims, there is also the potential for these predators to meet their contacts in person. Cyber predators can then physically abuse.

2.1 Always Handle Online Posts Carefully

Warn your children about some common tactics that online predators may use to lure them (these just a research and can appear in any number of variations). Ways predators approach and communicate with kids are:

- Let's go private
- Where's the computer in your house?
- When your father or family is going on vacation?

- You are my first love
- I can help you get a modeling job
- Please send your bold pictures
- You seem upset, tell me what's bothering you
- What precious things your family will buy this week?
- If you don't do that I'll show your parents the photos you've sent me
- I want to give you money please tell me your account
- We should meet in person, where do you live?

2.2 What can Parents do about Predators

Although many people online are honestly nice, predators may use flattery to try to start a relationship with a teen. This doesn't mean you need to be suspicious of everyone, but you should be careful. Internet safety for child depends on parents being aware of online risks and understanding how to help their children and teens avoid them. Parents should



encourage open communication and be diligent about explaining the dangers of online predators and inappropriate advances in any arena so children have an awareness of predators and dangerous situations. Children and teens should never be left unsupervised access to electronic communications. More important than blocking unpleasant material is teaching your children safe and responsible online behavior, and keeping an eye on their Internet use.

Microsoft recommends the following steps for parents to safe children from online predators.

- Talk to children and teens about online and offline predators and dangers.
- Spend time online together to teach your kids appropriate online behavior.
- Bookmark kids' favorite sites for easy access.
- Explore your children's recent search history to gain a better understanding of what to tell them to avoid.

- Understand privacy settings and read through privacy agreements before using any app.
- Adjust privacy settings and take advantage of internet safety tools such as NetNanny or SafeSearch.
- Keep the Internet-connected computer in a common area of the house, not in kids' rooms and try to sit with kids when online.
- Try to keep your kids email account accessible, requiring young child to use a family email account, and requiring teens to give their password.
- Microsoft advises parents to check all devices for pornographic materials and further investigation.
- Take your child seriously if he or she discusses an annoying online experience
- Watch for warning signs of a child being targeted by an online predator. These can include:
 - spending long hours online, especially at night
 - phone calls from people you don't know
 - unsolicited gifts arriving in the mail
 - your child suddenly turning off the computer when you walk into the room
 - taking away from family life and hesitancy to discuss online activities
- Talk to your children! Keep an open line of communication and make sure that they feel comfortable turning to you when they have online issues.



2.3 What can Children Do?

Children and teens can do a variety of things to protect themselves online:



- Don't post pictures or comments that are inappropriate. Avoid posts about drugs and alcohol, or those featuring nudity, racism, violence or threats.
- Get your friends to agree that none of you will post any comments or pictures that would hurt each other.
- Block anyone who posts harassing, threatening or inappropriate comments about you and inform them to parents or teachers.
- Be wary of new friends you meet through social media. They may be trying to get something from you.
- Don't talk about sex with anyone online. This is the easiest way for predators to harm children.
- Avoid in person meetings with someone you've only met on social media.
- Never use easy to understand password like your date of birth, school joining date, or password like 12345 or one password for your all online world.
- Never give your personal information, account number, home address, CNIC in a chatroom or online.

- Never download if someone emphasis to download something, and also never download anything from unknown sources.
- Also avoid screen names that have school symbol or logos in it.
- Use email filters to keep out communications from questionable sources.
- Be careful with screen names: don't use gender-specific names, don't use any erotic language and don't reveal personal information in screen names or profiles. This can put children at risk of not only predators, but identity theft.
- Avoid posting that you are going on vacation, or posting pictures while on vacation... until you are back home.

2.4 Public Wi-Fi and Online Predators

Public Wi-Fi seems to be a great blessing, since these free access points are available at restaurants, hotels, airports, and even random retail outlets, but it is actually a security threat in disguise. Children love to use free WI-Fi, but it is also a preferred spot of online predators. Hackers use various ways to steal users` data on public Wi-Fi. They track your online activities on the network and may send malware to your device while being on the same network. If you are using public Wi-Fi, make sure your select for an authentic one. Usually, predators create fake public networks by the names of well-known businesses, and if you won't be cautious, you can trap by them. Children can easily be trapped in public Wi-Fi predators.



Here are some potential tips for staying safe on public Wi-Fi networks.

- First, verify your Public WI-FI connection with authorize person.
- Avoid checking sensitive data, bank transactions on public Wi-Fi
- Discourage your child to play online games on public Wi-Fi.
- Try not to install any software program through public Wi-Fi, there's also the possibility it could be a malicious attempt to download malware onto your system.
- See the code https and not just http in a site's URL. This is a sign that it has an SSL certificate, showing it's a safe website to download or visit.
- Never install any Apps outside of the App store in public Wi-Fi.
- Turn off sharing from your device while you are on public Wi-Fi.
- Use a virtual private network (VPN) during the sensitive communication on public Wi-Fi network.
- Keep Wi-Fi off when you don't need it or you are don.
- Keep Wi-Fi off when you don't need it or you have completed your work.



3 Why Playing Online Games Isn't all Fun

Many parents warn their children about the dangers of drugs and alcohol. Fewer parents, though, know that they should also warn against so-called online-games that are so risky they can lead to injury or death. Pornography is often embedded in today's online games,



allowing kids to engage in virtual or simulated sex acts to accumulate more points. Some games exist for the sole purpose of simulating sex—virtual sex games are often free and easy to access for kids; these games allow kids to create an online identity to explore sexuality. According to Dr. Jill Manning,

"Parents need to understand how intricately linked the gaming industry and pornography industry are. More and more games have pornography embedded in them. If kids play online, that is a pornographer's heyday for marketing, and hooking young consumers."

Since predators target where kids play, it is no surprise that online games are the new frontier for sexual predators. They use online gaming to connect with children and target their next victim. The interactive nature of video games, where players participate in the on-screen action, parents can worry that this will affect children's behavior. This is particularly true where younger players experience more violent games not necessarily designed for their age group.

3.1 Shocking Stories about Online Games

Recently, there has been an alarming number of deaths based on challenges made popular on social media and the internet. These challenges and games give kids a sense of thrill without realizing the horrible consequences. For the safety of your children, it's important to make yourself aware of the details of these online games and challenges. Jennifer shu, MD says about these challenges, "they usually play in groups where there is peer pressure."

3.1.1 The Cinnamon Challenge

The cinnamon challenge is a viral internet food challenge. The objective of the challenge is to film oneself eating a spoonful of ground cinnamon in under 60 seconds without drinking anything, then upload the video to the Internet. The challenge is difficult and carries substantial health risks because the cinnamon coats and dries the mouth and throat, resulting in coughing, choking, vomiting, and inhalation of cinnamon, leading to throat irritation, breathing difficulties, and risk of pneumonia or a collapsed lung.



3.1.2 Fire Fairy

Fire Fairy is an online game targets younger children. It gives children dangerous instructions to turn on the gas in the stove at midnight when no one else is awake, and then go back to sleep. The game promises that they will wake up and become fire fairies. As reported by the Daily Mail, a five-year-old girl has already fallen victim to the game and suffered severe burns to her body when she thought she could be turned into a “fire fairy” as promised online.



3.1.3 RapeLay

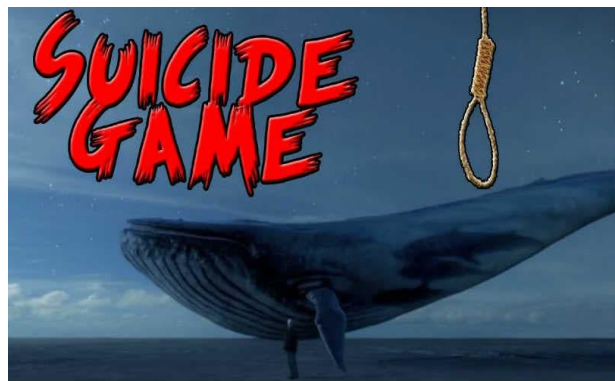
Another online game is RapeLay, which centers on a male character who walk rigidly and rape a mother and her two underage daughters. The complete story is too indecent that I can't even explain it here...

3.1.4 Mariam Games

In Mariam games, a child lost in the forest seeks players' help to find her way back to home. Within frightening audio and visual effects, the child asks players many personal questions such as 'Where is your home located?', and 'What's your Facebook account?' Players can advance to the next level only by answering the questions. Experts believe that the game seeks players' personal information that can be used for identity theft or other unlawful purposes (online predators).

3.1.5 The Blue Whale

The Blue Whale challenge, game is an online social media group where administrators ask children and teens to take on a series of challenges that end with them eventually killing themselves. It is reportedly responsible for hundreds of teen suicides worldwide. The 'challenge' starts with simple tasks such as watching a horror movie, and the level of 'hardness' increases as one keeps completing tasks. Finally, over a 50-day period, players have to commit suicide to 'win' the challenge. Administrators of the game are assigned to exact peer pressure on players, mostly young children and teens. Saudi Arabia banned a long list of popular games. The ban was in response to the deaths of a 13-year-old girl and a 12-year-old boy who reportedly killed themselves after playing "Blue Whale" social media game.



In the UAE, many video games are banned due to the promotion of nudity, violence, and negative image of Muslims. Games that are banned in this country are: Mass Effect, Dead Island, God of War, GTA, Dragon Age, Mafia 2, Godfather 2, Darksiders, and

Call of Duty 4: Modern Warfare. Similarly, the Pakistani authorities put a ban on Call of Duty: Black Ops 2 and Medal of Honor: Warfighter. The reason for this was showing the country in a negative light.

3.2 Parental Guide for Gaming

As we know that the impulse control and decision making part of children and teens are not fully developed, they don't understand the future consequences of today's actions. It means when children are dealing with unsupervised online games, they must need



parental or trusted adult guidance and supervision. Parents or guardians can do a variety of things to protect their children or family from the dangers of dark side of online games such as:

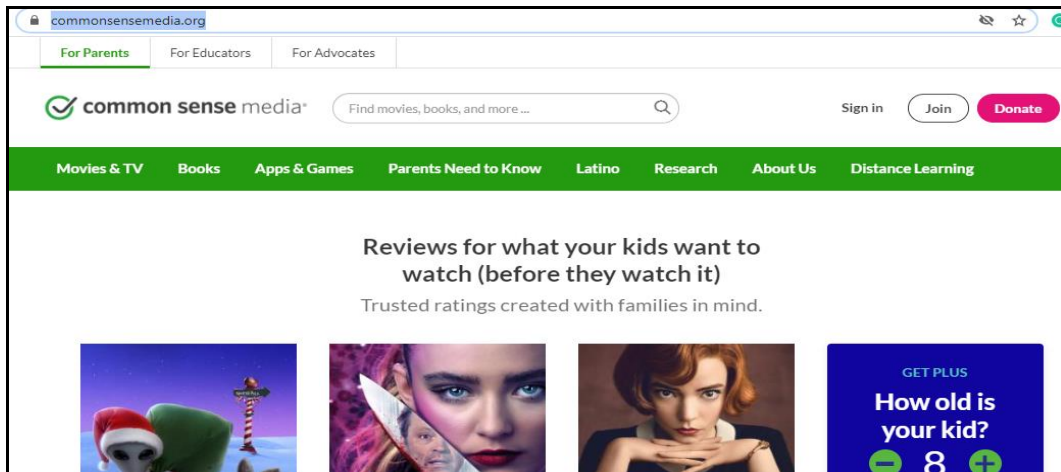
- Review the game to make sure it is appropriate.
- Check game ratings to see if it's appropriate for your child's age.
- Check to see if the game has moderators or features to report inappropriate behavior.
- Try to play online games with your child.
- Keep gaming equipment in a common area where you can supervise.
- Know the safety features for the game and equipment your child uses.
- Set safety features and parental control options on the video game gear.
- Set rules about how much time your child is allowed to play.
- Teach your child to never give out personal information while gaming.

3.3 How to Recommend Online Games

I highly recommend that parents first go through the review of a game, if they satisfy then allow it to their children to play. For this purpose I recommend the following free site to get the reviews of various games. The step by step procedure are as follows:

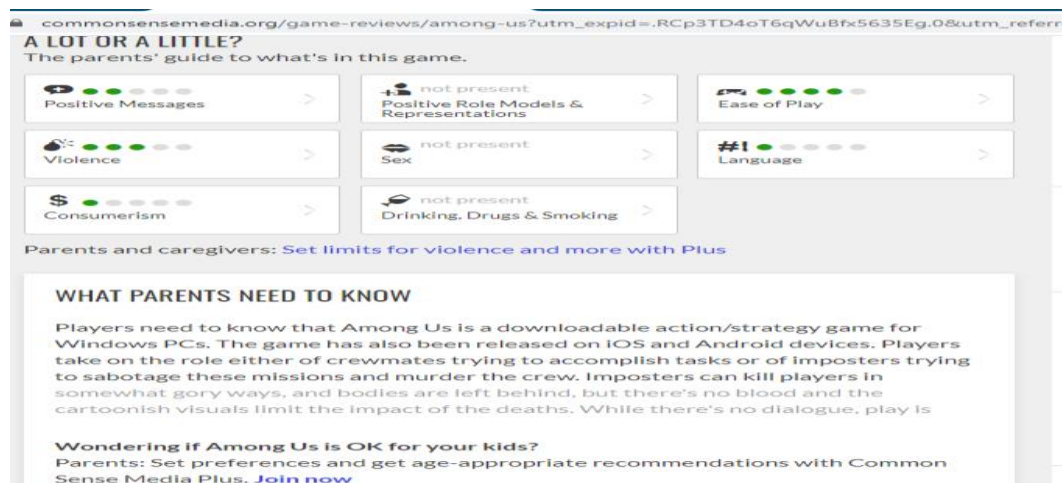
Step 1: Type on Google: <https://www.common sense media.org/>

Step 2: The following window will open



Step 3: write the name of any game in search box that you want to review.

Step 4: Scroll down the page you will find the review as:



4 Dangers of Cyberbullying

Cyberbullying is bullying that takes place over digital devices like cell phones, computers, and tablets. It can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share contents. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or nasty content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation. In other



words, it's anything that gets posted online and is meant to hurt, harass, or upset someone else for example:

- spreading lies about or posting embarrassing photos of someone on social media
- sending hurtful messages or threats via messaging platforms
- Impersonating someone and sending mean messages to others on their behalf.

When bullying happens online it can feel as if you're being attacked everywhere, even inside your own home. It can seem like there's no escape. If someone is already depressed or anxious, cyberbullying can make things much worse. The effects can last a long time and affect a person in many ways:

- **Mentally** — feeling upset, embarrassed, stupid, even angry
- **Emotionally** — feeling ashamed or losing interest in the things you love
- **Physically** — tired (loss of sleep), or experiencing symptoms like stomach aches and headaches



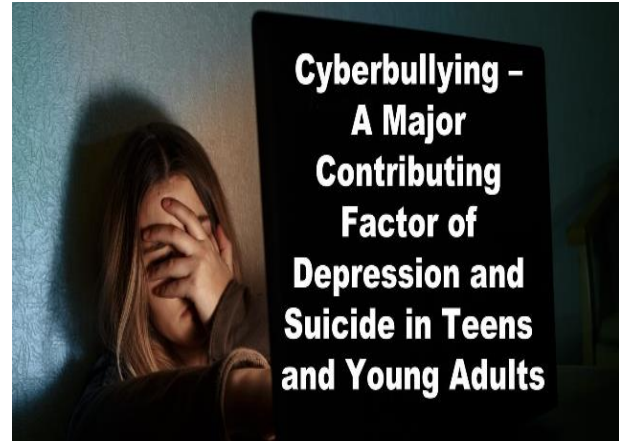
Cyberbullying increases the risk of suicide. Kids that are constantly tormented by peers through text messages, instant messaging, social media, and other outlets, often begin to feel hopeless. They may even begin to feel like the only way to escape the pain is through suicide. As a result, they may fantasize about ending their life in order to escape their bullies.

Cyberbullying can affect us in many ways. But these can be overcome and people can regain their confidence and health.

4.1 Signs Your Child is Being Cyberbullied

Cyberbullying is becoming a burning issue both for parents and teachers. Kids spend around 3 hours online and use cell phones 80% of the time, making it the most common medium for online bullying.

- No longer using the internet or checking their phone
- Showing stress when they get emails, texts or other alerts
- Withdrawing from family and friends
- Not wanting to go to social or school events
- Showing signs of low self-esteem, depression or fear
- Having declining grades
- Losing their appetite or having trouble sleeping
- Having suicidal thoughts



It is the parents' duty to teach your child how to stand up for cyberbully victims, few considerable actions should be as:

- Don't comment on posts that insult or harass others.
- Don't forward embarrassing photos or messages.
- Report cyberbullying to the website, app or concern authorities.
- Support the victim, be a good friend and show cyberbullies you won't join their harassment.
- Tell a teacher at school if it involves a classmate otherwise tell to parents.
- The most important is, let the children clearly know they will never do anything online, which will shamefully for them and others.

4.2 Parental Guide for Cyberbullying

If a child is expressing anger or anxiety after going online, it might be one of the signs he/she is being cyberbullied. Cyberbullying is the same as traditional bullying but if traditional bullying stops, when the school ends, for online bullying there is almost no escape. Unfortunately, many kids irritate and harass each other using the internet via computers and smartphones. Researchers find that the cyberbullying victims are 3 to 9 times more likely to consider committing suicide and 45% of children admit they have experienced bullying online. The more alarming facts are, only 2 in 10 victims inform their parents or teachers of online bullying.

- **Discussion:** Be patient and ask a child about the problem in general: what is cyberbullying, does he/she know someone who is being bullied, what children should do if notice acts of bullying.
- **Success Stories:** Tell your child the success stories of shining stars, and let them know how bad comments people pass about them but they pay no attention. This trick defuses the intensity of bullying in child's minds.
- **Monitoring:** Always monitor your child online activities, this habit can safe him from many online evils. In the next pages, I will suggest you the best online monitoring tools.
- **Awareness:** Many people still unaware about the severity of Cyberbullying. School should conduct seminars and workshops to discuss cyberbullying, and discourage the initiators.
- **Careful about Posting:** Before sending anything related to yourself to your best friend or family member, consider if this is something you would want others to see. Bullies can use your post to make your life unhappy. Don't post anything that can compromise your reputation.
- **Google yourself:** Periodically search your name on search engine and see if any personal information or photos come up. If you find something that can be used by cyberbullies to target you, take quick action and have it removed.
- **Don't be a cyberbully:** Treat other as you want to be treated. If you are evil to others online, you must deserve the same behavior for yourself.
- **Use PC:** Try not to logging too much with public computer, always use personal computer for online activities.
- **Report** – If a classmate is cyberbullying, report it the school. You can also contact app or social media platforms to report offensive content and have it removed. You can also report it to the concern authorities as I have mentioned in this guide.

5 Social Media Safety for Your Children

Nearly all social networking sites only allow users aged 13 and above, to create an account with false information is violation. This age limit has been described by the Children's Online Privacy Protection Act (COPPA). The existing social media sites can bring risks for your child. Without meaning to, kids can share sensitive information which can create cyberbullying, online predators

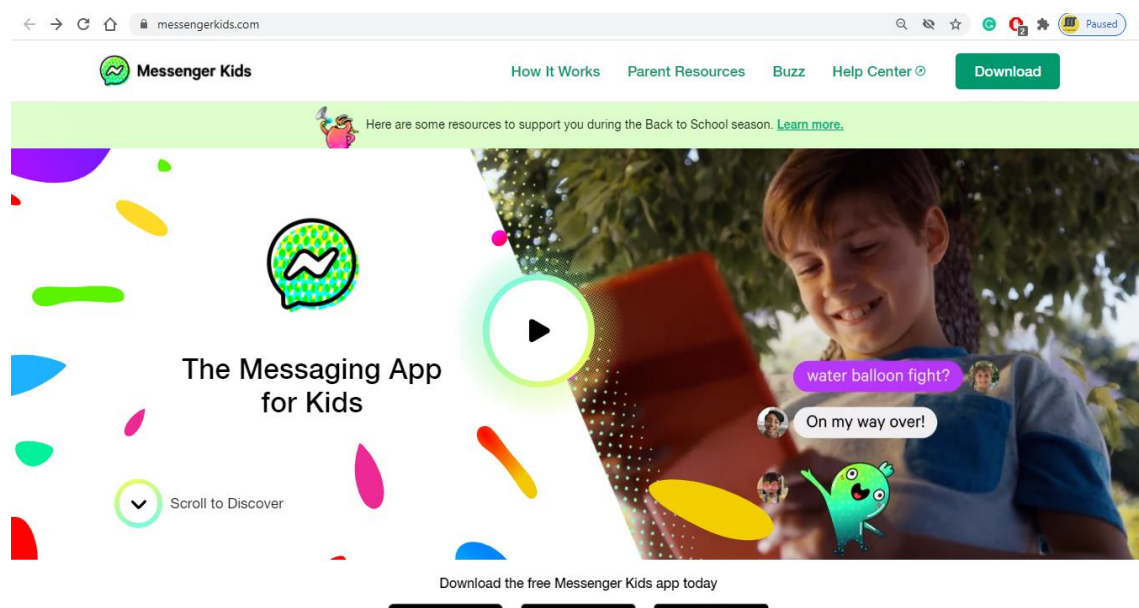
and many other social issues. They would also receive unwanted online advertising that might be inappropriate for their age. They may contact online by someone they don't know before, which can make them feel scared or uncomfortable. We should explain to our children about the dangers of existing social media, and emphasis to use social media that specially designed for the children or young teens.

5.1 Social Media for Children and Teens

If you're looking to introduce your child to social networks and want peace of mind, look no further. I know some of the most popular and secure sites for your kids and teens, as:

5.1.1 Messenger Kids

Messenger Kids is Facebook's offering which works as an alternative to its more adult-centric messaging app and platform. It functions in much the same way its full-fledged older sibling does, allowing children to message and video call their peers.



The main difference is that parents remain in control through Messenger Kids Parent Dashboard. The dashboard allows you to review your child's chat and contact histories as well as have an overview of whom they reported or blocked. It will also give you access to the most recent videos and photos they sent and received, with the option to remove and report anything you deem inappropriate. And you can even download your child's information from the app and remotely logged them out of the app on any device.

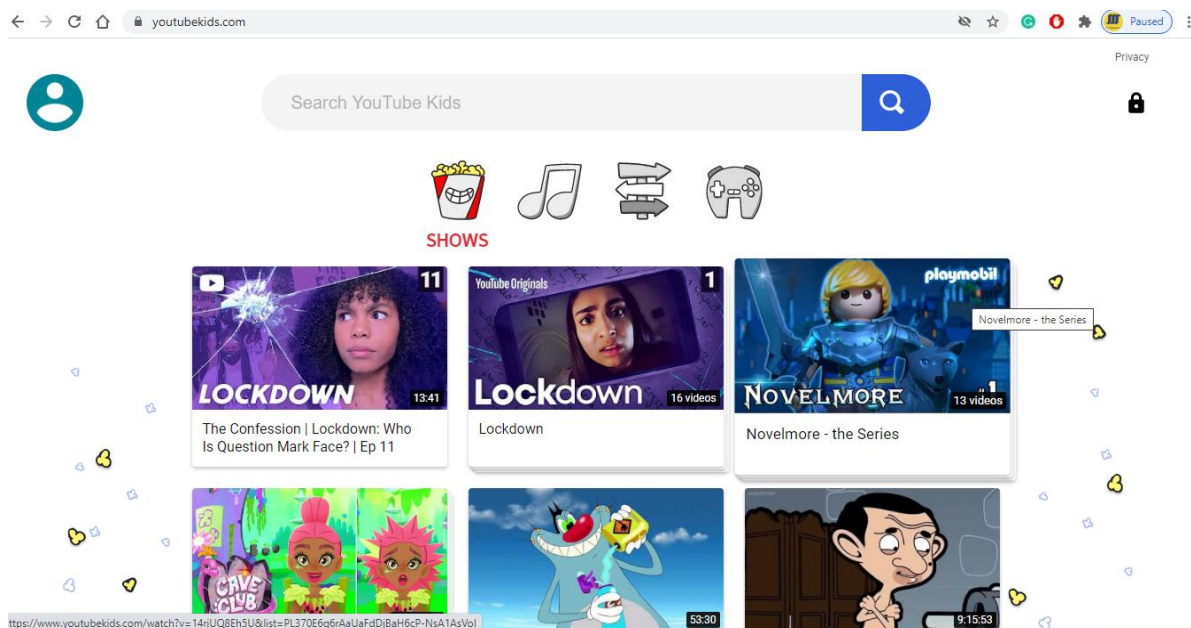
Website Link: <https://messengerkids.com/>

Note: To learn how this social media works simply go to the site, <https://messengerkids.com/> and click on how it works (<https://messengerkids.com/how-it-works/parent-dashboard/>) then you will find a video that tells you the complete features about the site in a very simple way.

5.1.2 YouTube Kids

YouTube Kids is a leading destination for video, developed by YouTube, aimed directly at children. Technically, the app is a portal to the main YouTube service and uses an algorithm to filter out the adult stuff and funnel the kid stuff to the app so that your children can only access safe search. It provides a variety of the services for children, with carefully selections of content, parental control features, and filtering of videos deemed inappropriate viewing for children. YouTube Kids gives your family an easy way to watch their favorite shows, or explore anything that captures their imagination. It's free, simple to use, and full of family-friendly videos. YouTube Kids will provide no answer of any abusive or vulgar searches.

Main concern: Finding kid-friendly YouTube videos, and blocking ads and links



At the top of YouTube Kids, you'll see icons for video content by category:

- Shows includes kid-friendly programming from popular YouTube creators, family media networks and new and nostalgic characters.

- Music includes nursery rhymes, kid-friendly covers, dance tutorials and sing-alongs.
- Learning includes content to promote fun, active learning: from ABCs and 123s, to science experiments and language learning.
- Explore includes content that inspires children to explore the world around them, develop new hobbies, and explore topics they're interested in.
- Gaming includes content featuring kids' favorite video games and gamers. This category is shown only when the Older content setting, which is only available in certain countries.

Website Link: <https://www.youtubekids.com/>

Note: You can easily search and install YouTube Kids from Google Play Store.

5.1.3 Google for Kids Search Engine

Safe Search Kids is powered by Google for filtered search results. Safe Search Kids is a custom search engine powered by Google to allow everyone to search the internet more safely. We use Google's Safe Search features with additional filtering added to block potentially harmful material.



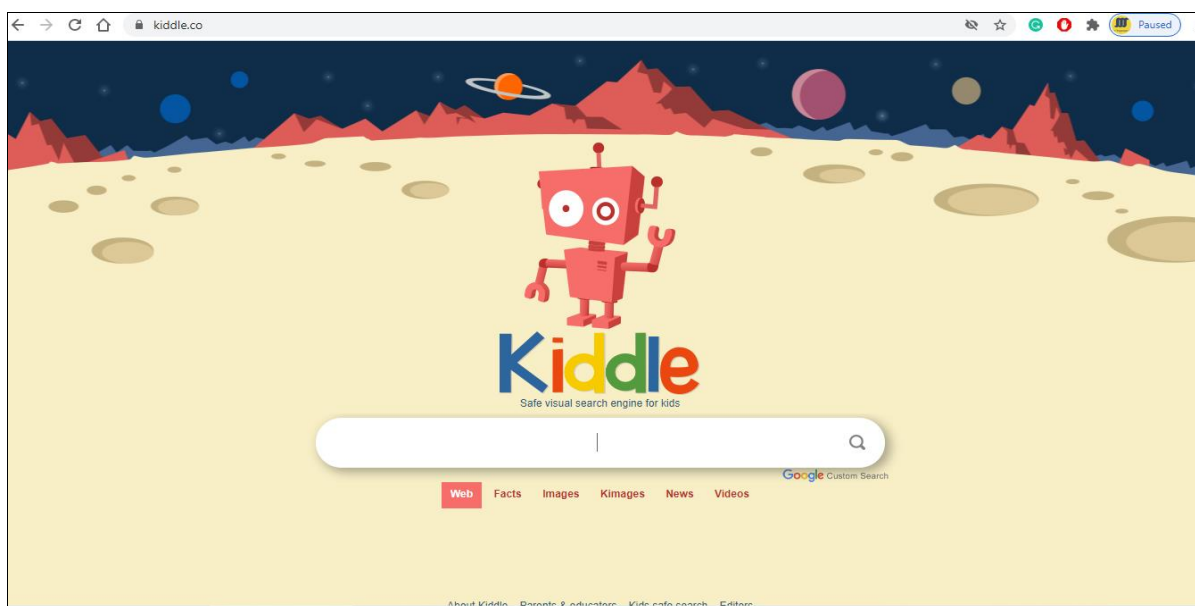
Safe Search Kids filtering tools provide a way for parents at home and teachers in school to allow their kids to research the internet with safe boundaries. No matter what browser you use, strict filtered results are always on.

That being said, the easy way to activate Google for kids with safe search is to bookmark this website for kids at home and in school.

Website Link: <https://www.safesearchkids.com/>

5.1.4 Kiddle for Kids

Kiddle is a web search engine and online encyclopedia emphasizing safety for young children. The user enters topics in the search toolbar, and Kiddle returns and ranks its findings, and pushes child-safe content higher in its search results. It finds the search articles and categories to help you research different topics for school homework help, homeschooling and general education. With the secure searching, Kiddle is also useful for school assignments, homework and project concept. In Kiddle Facts tab, you can find interesting articles, concepts and many more things related to children education. It could be a valuable resource for the teachers to find almost all field of education.



All content from Kiddle encyclopedia articles (including the article images and facts) can be freely used for personal and educational purposes.

Website Link: <https://www.kiddle.co/>

6 How to Report Cyber Crimes in Pakistan

To protect yourself against cybercrimes you must first know what type of cybercrimes there are. The internet is a complex infrastructure where cybercriminals create about 57,000 scam websites every week. The following are the list of the most popular cybercrimes.



- **Identity Theft** scams gain access to your credit card or banking account information may use that information to make purchases in your name.
- **Phishing** scams is a practice of a cybercriminal or hacker attempting to obtain sensitive or personal information from a digital user.
- **Online Harassment** can consist of threats sent through email, instant message or through a social network message/post. Harassment can also be found to result in cyberbullying, as you may have witnessed recently in the media where a 13-year-old kid committed suicide from being bullied online. Our suggestion for handling harassment online is to immediately report any activity out of the ordinary before it gets out of hand.
- **Cyberstalking** is known to continually harass victims it goes long to monitor online activities. Cyberstalkers may contact a victim's colleagues, friends and other online contacts in an effort to slander them or extract personal information from them.
- The **invasion of privacy** is basically the act of someone attempting to intrude on a person's personal life. If you ever suspect someone invading your privacy, you can simply file a report.

In any of the above cases, you should always have the proper computer security applications installed and updated on your computer which may include a trustworthy anti-spyware or anti-virus program. Having security software installed and running on your system will ensure that you are protected from known threats that can lead to any of the above situations and help protect you and your child against cybercrimes.

Pakistan has been included in the list of the fastest-growing countries that are using the internet which also opens the doors for the fact that cybercrime is increasing as well. However, if you know someone being harassed online or are a victim yourself, here's are different ways you understand to do.

6.1 Register a Complaint through FIA

Simply write down your application (in English or in Urdu), narrate your complete problem, provide as much evidences, details as you can and send it to FIA National Response Center for Cyber Crimes (NR3C). FIA is a law enforcement agency dedicated to fight cybercrime and technology based crimes in Pakistan.

Website Link: <http://www.fia.gov.pk/en/NR3C.php>

How to Get Update on Complaints:

You can email (helpdesk@nr3c.gov.pk) or contact them on 051-9106384 or Mobile no: 03366006060 for any queries against your complaint and updates.

Register complaint against cyber-crimes by filling form online: Go to this URL and submit your application online: <http://www.nr3c.gov.pk/creport.php>


Register complaint against cyber-crimes with Email: Write an application with all possible details and your complete credentials (Name, Address, CNIC, and Contact No.) and email it to this email-address: helpdesk@nr3c.gov.pk

Register complaint against cyber-crimes by writing hard-copy application: Write an application with all possible details and your complete credentials (Name, Address, CNIC, and Contact No.) and send the application to this address:

Director NR3C-FIA, National Police Foundation Building, 2nd Floor, Mauve Area, G-10/4, Islamabad.



ABOUT US DEPARTMENTS COMPLAINTS MOST WANTED PRESS RELATED



LEADING THE NATIONAL EFFORTS TO COMBAT CYBER CRIMES

NATIONAL RESPONSE CENTRE FOR CYBER CRIMES

Investigation/ Prosecution of Hi-tech Crimes | Forensics Analysis of Digital Devices | Research & Development
Digital Crimes Investigations | Information System Security Audits | Technical Trainings
Advisory Role on Information Security | Capacity Building and Awareness of Government Departments and Academia

National Response Centre for Cyber Crimes

INTRODUCTION

National Response Centre for Cyber Crime (NR3C) - FIA is a law enforcement agency dedicated to fight cyber crime. Inception of this Hi-Tech crime fighting unit transpired in 2007 to identify and curb the phenomenon of technological abuse in society.

National Response Centre for Cyber Crime (NR3C), is the latest introduction to mandate of the FIA, primarily to deal with technology based crimes in Pakistan. It is the only unit of its kind in the country and in addition to the directly received complaints also assists other law enforcement agencies in their own cases.

NR3C has expertise in Digital Forensics, Technical Investigation, Information System Security Audits, Penetration Testing and Trainings. The



LATEST NEWS

JULY 02,2020
FIA submits interim report to SC about life threat hurled to justice is | [READ MORE](#)

JUNE 12,2020
Senate panel discusses social media campaign against Zardari | [READ MORE](#)

JUNE 10,2020
FIA wants dismissal of plea against US blogger | [READ MORE](#)

JUNE 04,2020
Reporting harassment a click away | [READ MORE](#)

...gives an edge to professionals to understand and excel in their respective fields. NR3C over years has trained around thousands of individuals of academia, law enforcement agencies, judiciary, police academy, intelligence agencies etc. Trainings disseminated in relation to digital forensic comprehension of interpreting forensic reports, evidence extraction methods, laws application to judicial community. 12, 458 individuals from all walks of life ranging from a 6 grade kid to a decorated officers have been trained by NR3C to serve the purpose cyber crime mitigation.

CYBER CRIME

Any activity commissioned via computer, digital devices and networks used in the cyber realm, and is facilitated through the internet medium. It can include the distant theft of information belonging to an individual, government or corporate sector through criminal tress-passing into unauthorised remote systems around the world. It includes from stealing millions of rupees from online bank to harassing and stalking cyber users.

Cyber Crime also includes sending viruses on different systems, or posting defamation messages. Commission of cyber crime can be:

- Cyber crime has now surpassed illegal drug trafficking as a criminal moneymaker
- Somebody's identity is stolen every 3 seconds as a result of cyber crime
- Without a sophisticated security package, your unprotected PC can become infected within four minutes of connecting to the Internet

MAJOR ONLINE ACTIVITIES

In Pakistan, internet users range from 10% to 16% of the overall population

- Social networking
- Online banking
- Internet surfing
- Audio & video communication
- Entertainment
- Online shopping
- Map directions / GPS
- Online auction
- Information sharing
- Medical assistance
- Online games

CYBER CRIME CATEGORIE

- Hacking
- Computer viruses and worms
- Identity theft
- Malicious Software
- Cyber Gossiping
- Intellectual property rights
- Cyber Stalking
- Money Laundering
- Financial fraud
- Denial of Service attack
- Digital Piracy
- Electronic Terrorism, Vandalism and Extortion

CYBER CRIME CATEGORIES

OVERSEAS PAKISTANIS COMPLAINT CELL


OVERSEAS PAKISTANIS FOUNDATION

STAFF WELFARE

PENSIONER CELL

CAREER OPPORTUNITIES

PRESS RELEASE



The screenshot shows the 'Complaints Registration Form' on the website complaint.fia.gov.pk. The page header includes the FIA logo and the text 'FIA FEDERAL INVESTIGATION AGENCY, MINISTRY OF INTERIOR, GOVERNMENT OF PAKISTAN'. A navigation menu contains links for ABOUT FIA, WINGS, PROJECTS, COMPLAINTS, MOST WANTED, PRESS, and RELATED. The form itself is titled 'Complaints Registration Form' and includes a note: 'All fields marked with * are mandatory.' The form fields are as follows:

- Name*: Full Name
- Gender: Male (dropdown menu)
- Telephone No. 1*: Telephone/ Mobile No.
- Telephone No. 2: Telephone/ Mobile No.
- Email Address: Email Address
- Occupation: Student (dropdown menu)
- Postal Address*: Postal Address
- City Name: Abbottabad, Abbottabad (dropdown menu)
- Crime Details*: Brief Crime Details with URL's and Mobile No. of the alledged person.

At the bottom of the form, there is a checkbox for 'I affirm that all the information I have provided on this form is correct to the best of my knowledge.' and a 'Submit Complaint' button.

6.2 File a Report via IC3

The FBI's Internet Crime Complaint Center (IC3) provides the public with a reliable and convenient mechanism to report Internet crime. It accepts online Internet crime complaints from either the actual victim or from a third party to the complainant.

The IC3 created the Recovery and Investigative Development (RaID) Team in 2019 to partner with financial and law enforcement investigators to dismantle money mule organizations. RaID comprises two groups: the Recovery Asset Team (RAT) and the Money Mule Team (MMT). While the RAT is primarily focused on financial recovery, the MMT performs detailed analysis and research on previously unknown targets to develop new investigations. The RAT, which was established as a standalone team in 2018, completed its first full year of operation in 2019, assisting in the recovery of over \$300 million lost through online scams, for a 79% return rate of reported losses. With the release of the 2019 Internet Crime Report, the FBI wants to remind the public to immediately report suspected criminal Internet activity to the IC3 at ic3.gov.

Website Link: <https://www.ic3.gov/>



THE END