

**PARENTS
VERSION**

STAYING SAFE ONLINE



**A GUIDEBOOK TO HELP PARENTS
TEACHERS AND TEENS NAVIGATE
ONLINE SPACES**

By Camila Gomide, Imaan Haque, Suzanne Lea, and Vaibhavi Maske

#TOGETHER

#TOGETHER

#T



This Guidebook was made in collaboration between Red Dot Foundation and Red Dot Foundation Global

By Camila Gomide, Imaan Haque, Suzanne Lea, and Vaibhavi Maske

Edited by ElsaMarie D'Silva, Andrea Adams and Camila Gomide

Design by Nishanth J & Laura Bertolato Silva

SUMMARY

<u>01</u>	<u>About Red Dot Foundation</u>
<u>02</u>	<u>Meet our Characters!</u>
<u>04</u>	<u>Glossary</u>
<u>06</u>	<u>Gaming</u>
<u>09</u>	<u>Understanding 21st Century Technology: A Journey Through Time</u>
<u>12</u>	<u>Online Sexual Harassment</u>
12	The Street Harassment Slippery Slope
13	Online Child Abuse
14	Online Harassment in Gaming, Virtual Reality, & the Metaverse
<u>15</u>	<u>Censorship Vs. Safety</u>
<u>16</u>	<u>Parent-To-Parent/ Teachers advice</u>
<u>17</u>	<u>Reporting on Safecity</u>
<u>18</u>	<u>Taking Action to Stop Online Abuse and Harassment</u>
<u>19</u>	<u>Support Us</u>

About Red Dot Foundation

Red Dot Foundation Global is a 501(c)(3) organization that has been crowd mapping sexual and gender based violence for the last eight years on its globally awarded reporting platform – Safecity. The dataset on the app is crowdsourced anonymously, meaning that each user can anonymously and safely report incidents. The idea is to make this data useful for individuals, local communities and local administration as a way to identify factors that cause behavior that leads to violence and work on strategies for solutions. Red Dot Foundation Global works at the intersection of gender, technology, communications, data and urban planning, and Safecity is its flagship program.

How to Use This Guidebook

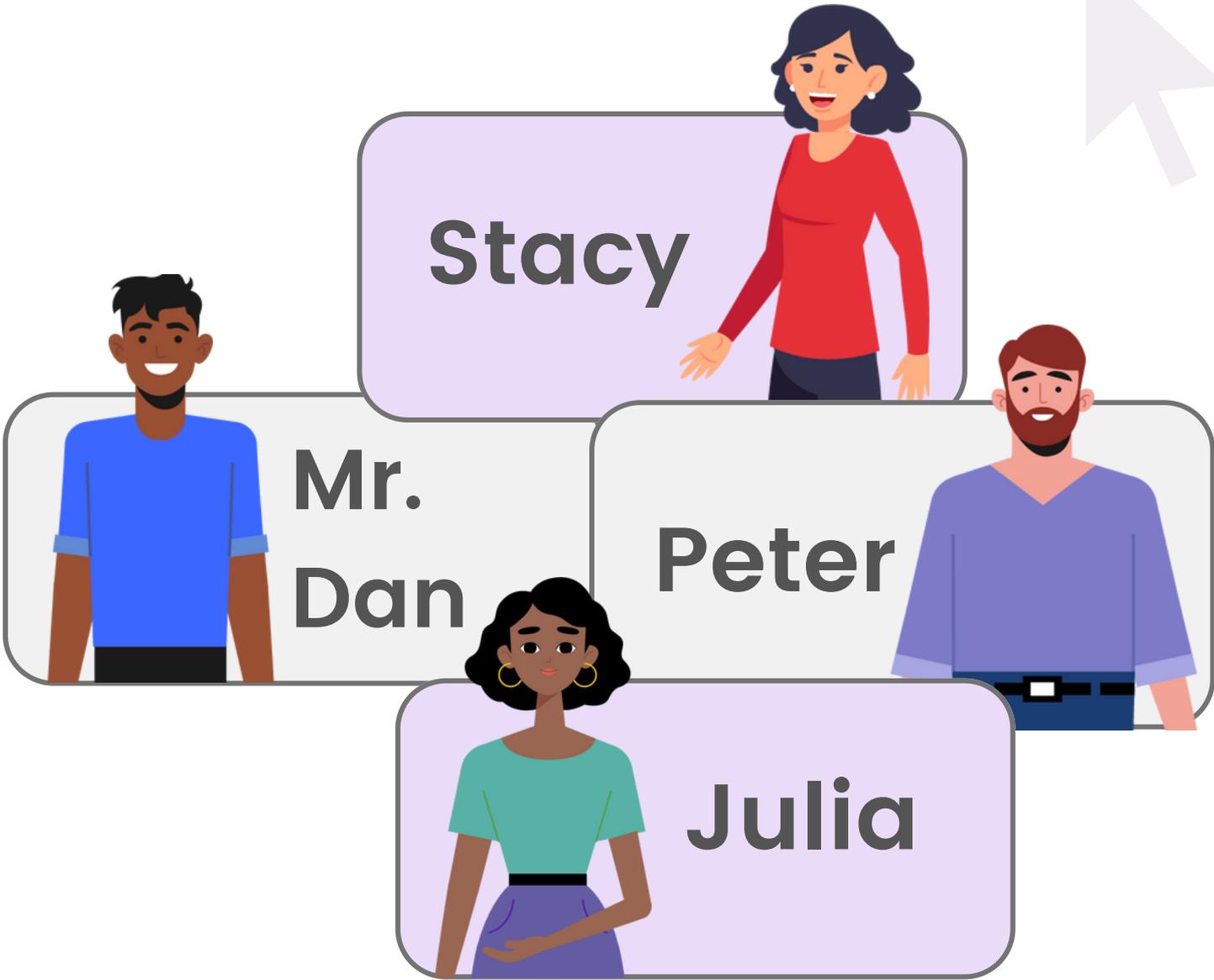
Use this guidebook as a tool full of important definitions, suggestions, and advice all about online safety for children of all ages.

This guidebook not only presents data, and a glossary of terms to help parents and educators stay on top of technology and trends, but it hopes to provide a resource to help you stay educated about online safety for any and all children in your life.

It's important to note that while this guidebook is a valuable tool, we suggest you use it as a general manual, rather than strictly follow it. Technology is ever changing, and not every situation calls for the same type of action. So use this book as a starting point for having informed conversations with children around you about online safety, and know that there are resources available all around to help in any circumstance. As technology changes, we will try our best to evolve with it, and will produce updated versions of this guide as needed.

Your first priority online should always be your personal safety and the safety of the children in your lives. It's important to know and understand your rights in the digital space. If you or anyone you know is affected by online abuse and needs support, you can share any incident of harassment anonymously on [Safecity](#).

Meet Our Characters



Stacy: The Online Safety Assistant

"Hey! My name is Stacy, your online safety assistant, and I will be your guide throughout this book! You'll find me in page corners, giving you more information about the different topics you'll learn! So, whenever you see a text box with the words "Keep an Eye Out" or "Did You Know", get ready to learn much more about curiosities and statistics!"

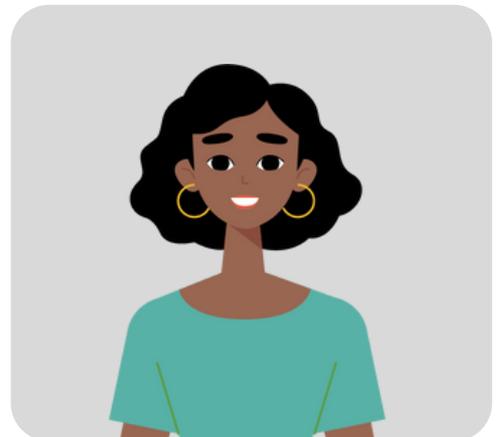


Mr. Dan: 6th grade English teacher. Students go to him if they need advice

"Greetings! My name is Daniel, but my students call me Mr.Dan. I am a 6th grade teacher and sometimes I find it challenging to guide students on internet safety. My students love to play with each other online, but I don't understand half of the terms that they use. I am excited to know more about terminology, so I can help my students better".

Julia: A working mom of 2, she has a son in grade 4 and a daughter in grade 7, worried about online safety when she isn't with her kids.

"Hey there! I'm Julia, Mariana's and Pietro's mom! I work full time as a financial advisor and rely on the school and extracurricular activities to keep my kids busy during the day. In the mornings and evenings, I try to educate my kids on what type of videos they can watch on social media, but I worry about what type of content they consume when I am not around. I am hoping to get some more information on how to educate them for when I am not around".



Peter: A stay-at-home dad who's 3 kids, ages 7, 9, 12, are super tech-savvy and he's worried because he doesn't always understand what they are doing online.

"Hi! My name is Peter and I am a stay at home dad to my three boys: Andre, Max and Thomas. They are in that phase where they spend more time playing games online than playing outside. Even though I dedicate my days to them, I feel like an outsider because when they have conversations I have no clue of what they talk about. I hope to understand more, so I can connect better with my kids!".

GLOSSARY



We understand that navigating the world of virtual reality, gaming, and the metaverse can feel overwhelming and confusing. To help you understand what all of these concepts mean, I have highlighted some important terms and phrases below.

Sexual Harassment:

Sexual Harassment: Sexual Harassment (SH), occurs when individuals (of any gender) are targets of unwanted sexual comments, gestures, or actions because of their actual or perceived gender, gender expression, or sexual orientation.

Sexual harassment can also happen in different settings and locations, such as in public spaces (on public transportation, at a park, inside a market), in private spaces (at home, at school, or at work), and also online.

SH can be divided into three main categories: gender harassment; unwanted sexual attention; and sexual coercion.

GENDER HARASSMENT

Refers to all forms of verbal and non-verbal behaviors that insult, and are hostile to others due to their gender. Gender harassment also includes making obscene sexual gestures, flashing, showing sexual objects at work, texting or emailing coworkers inappropriate sexual content, as well as sexist and heterosexist language and insults.

UNWANTED SEXUAL ATTENTION

Can be described as making unwanted suggestive comments about someone's body image, catcalling, and spreading sexual rumors or sexualized images of someone without their permission. Unwanted sexual touching can also be considered unwanted sexual attention

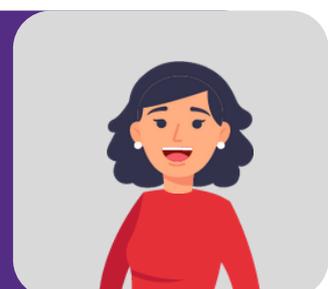
SEXUAL COERCION

Refers to requiring sexual contact or sexual favors as a condition to receiving any type of reward, such as a job promotion, grade or good evaluation.

Did you Know...

Sexual violence is a spectrum of abuse. We divide it into three main categories: verbal, non-verbal and physical.

- Non-verbal: Staring/Ogling, Taking pictures, Indecent gestures.
- Verbal: Commenting, Catcalls, Sexual invites, Online Harassment.
- Physical: Touching/Groping, Stalking, Sexual Assault, Rape.



Online Sexual Harassment

Cyber Stalking

Using any form of electronic communication to follow or attempt to contact or interact with someone, despite a clear indication of disinterest from that person.

Cyberbullying

The use of electronic communication to bully a person, typically by sending messages of an intimidating or threatening nature.

Doxxing

Revealing another person's personal information without their consent, including their full name, home or office address, phone number, or any other identifying details.

Online Impersonation

When someone uses your personal information – your electronic signature, your password, or anything that's identifiably yours – without your consent.

Concern trolling

Can be a bit tougher than some of these other types of harassment to define and identify, but essentially, it's expressing concern disingenuously, pretending to care but in fact using phony support to criticize or undermine.

Flaming

Attacking another person online by posting disrespectful comments about them, often with hostile language. This can include character assassination, posting lies, hurling insults, or other such aggressive behaviour.

Trolling

Deliberate action, (by a Troll – noun or adjective), of making random unsolicited and/or controversial comments on various internet forums with the intent to provoke an emotional reaction from unsuspecting readers to engage in a fight or argument.

Catfishing

A fake or stolen online identity created or used for the purposes of beginning a deceptive relationship. In other words, someone who makes a fake account of someone on social media (Instagram, Facebook, Tinder) to lure others into a relationship with a false identity.

Self-Generated Child Abuse:

Generated by abusers coercing children to create and upload sexual content from their own homes via webcams on laptops and desktops.

Grooming

When someone builds a relationship, trust and emotional connection with a child or young person so they can manipulate, exploit and abuse them.

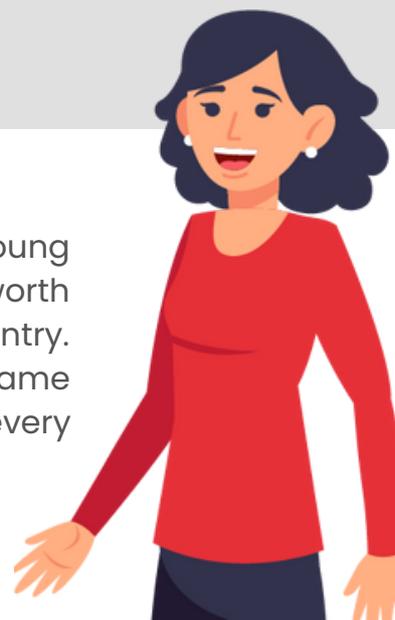


Online Sexual Harassment: Online harassment can appear in many shapes and forms. Online harassment is any type of targeting of individuals or groups on various online platforms and in virtual spaces. This means that online harassment can happen via email, social media platforms such as Facebook, Instagram, Twitter, and TikTok, as well as online messaging platforms such as WhatsApp. It also includes comment sections and publishing another individual's private information, such as a home address.

Social Media: Websites and applications that enable users to create and share content or to participate in social networking. Some examples are Facebook, Instagram, Snapchat, Twitter, Tiktok, and Discord.

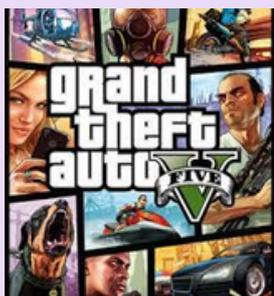
GAMING

Gaming is one of the most popular activities among young adults. In the United States alone, the gaming industry is worth nearly \$50 billion, with over 191 million gamers in the country. This is mimicked across the world as well, with video game engagement and consumption skyrocketing with every generation. Some of the most popular video games are:



Minecraft:

Video game in which players create and break apart various kinds of blocks in three-dimensional worlds. The game's two main modes are Survival and Creative. In Survival, players must find their own building supplies and food. They also interact with block-like mobs, or moving creatures. In Creative, players are given supplies and do not have to eat to survive. They also can break all kinds of blocks immediately. Usually played via a computer console, players can connect to thousands of Minecraft online games (servers), some of which involve battling other players.



Grand Theft Auto V:

Grand Theft Auto V is an action-adventure game played from either a third-person or first-person perspective. Players complete missions—linear scenarios with set objectives—to progress through the story. Outside of the missions, players may freely roam the open world. Played via consoles such as XBOX or Playstation, users can invite friends to play together virtually.



Fortnite:

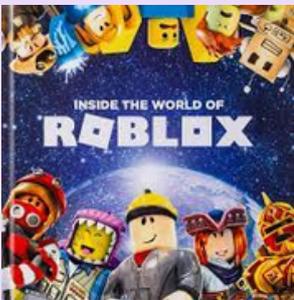
A world of many experiences. Players create islands and compete in teams to conquer other teams' islands. Players can hang out with friends on an island that someone else created, or save the world by taking down hordes of monsters with others.

GAMING



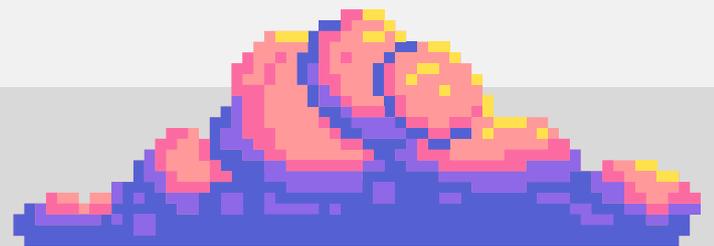
League of Legends:

One of the world's most popular video games. Team-based, with competitive game mode based on strategy and outplaying opponents. Players work with their team to break the enemy Nexus before the enemy team breaks theirs. It is a complex game which involves both high-level strategy and fast-paced gameplay.



Roblox:

Online platform where users go to play games. Roblox is not a game, it is a place where people play games made by other developers. What makes Roblox different from anything else in the games industry – including a storefront like Steam – is that all the games are made by its users.



READY TO
KNOW MORE?

START

VIRTUAL REALITY

Technology used to create artificial environments which are experienced through sensory stimuli (such as sights and sounds) provided by a computer and in which one's actions partially determine what happens in the environment. The difference between Virtual Reality (VR) and a computer game, is that VR allows the user to feel like they are inside the virtual world. This feeling is generated by users being required to use goggles, headsets, gloves, or bodysuits. For instance in a typical VR format a user wears a helmet with a stereoscopic screen and views animated images of a simulated environment.



AUGMENTED REALITY

Similar to Virtual Reality, augmented reality (AR) is a technology that provides users with an artificial environment that surrounds the user. However, augmented reality adds those digital elements through smartphone cameras, instead of requiring special equipment. One of the most common examples of augmented reality is the game Pokemon Go, and Instagram or Snapchat filters.

ARTIFICIAL INTELLIGENCE

Type of computer science that leverages computers and machines to mimic the problem-solving and decision-making capabilities of the human mind. One common example of artificial intelligence is companies, often banks, who use chatbots (when you chat with a machine) to solve a problem.



METaverse

Owned by Mark Zuckerberg, the Metaverse employs the use of virtual reality, augmented reality, artificial intelligence and others to create a 3D digital world that mimics the physical world. In other words, the Metaverse is an open, shared, and persistent virtual world that offers access to the 3D virtual spaces, solutions, and environments created by users.

DATA

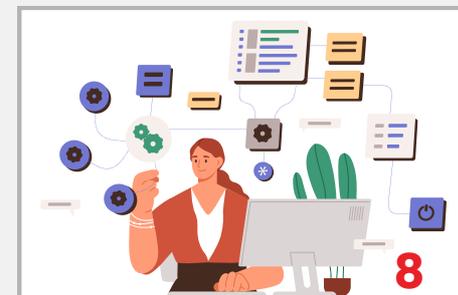
Facts and figures, or information that's stored in, or used by a computer. An example of data is information collected for a research paper, or as simple as an email.

TECHNICAL CENSORSHIP

Unavoidable side effects of safety controls. It is an automated filtering system that spots blacklisted words and flags the posts, regardless of whether the post context was harmful or not.

BIG DATA

The exponential growth and availability of information alongside the growing capacity of humans to analyze it. Big Data is also generally collected by large social media platforms, mainly Facebook. The information collected through Big Data is used by advertisers to target specific products or services to a certain audience.



Understanding 21st Century Technology: A Journey Through Time

Web 1

The beginning of the internet. In this era, the internet was a virtual encyclopedia, where users could search for information. All this information was centralized on certain platforms.

1980

During the '80s we saw an increase in personal computers or PCs around the world as Microsoft and Apple began their fight over who would be the best operating system.

1998

Google opens its workspace in California, and draws us in as we no longer have to wait for answers to our burning questions.

1974

The first personal computer, the Altair, was now available in our homes. This year the internet also came into existence with the help of Vinton Cerf and Robert Kahn who produced the TCP/IP (Transmission Control Protocol/Internet Protocol).

1990

In the 90s, cell phones are taking the world by storm, and more and more individuals have access to the internet through PCs, desktops, and the first laptops.



I remember when I got my first phone, it was so heavy, it was hard to carry it around!

Web 2

The era of social media, now users can interact with each other and create content that is available through blogs, and platforms such as Wikipedia, and YouTube.



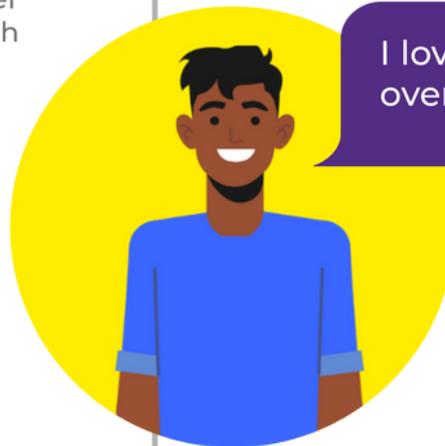
2004

Facebook is launched, taking over MySpace, allowing us to engage with people around the globe, and forever changing the way we interact with others.



2000

Cell phones are more common than ever with the advent of Blackberrys, the iPhone, and the fact that wifi is more publicly available.

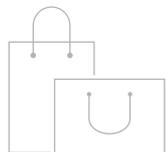


I love Facebook! I have over 100 friends!



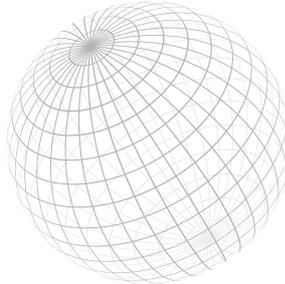
2010

Launch of Instagram, allowing people to share photos and videos virtually. Teens start to report being targets of cyber bullying.



2012

Ecommerce sales reach \$1 trillion worldwide, and the app Snapchat is released, including Artificial Intelligence and Artificial Reality features.



2016

The number of internet users reach 3.4 Billion people



2018

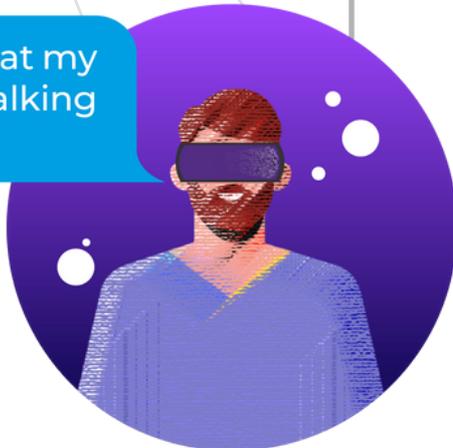
Facebook faces largescale trouble regarding data safety due to the scandal of Cambridge Analytica

Web 3



- The future of Internet
- Decentralized data usage, now the user owns their data.
- There's no company behind online platforms
- Beginning of cryptocurrencies and blockchain technology

Ooh so that is what my kids are always talking about!



Online Sexual Harassment

In this day and age, we are more connected than ever. The internet is an information superhighway that has brought us closer to each other, making communication extremely accessible and instant. But as we know, there are several downsides to this ease of access.

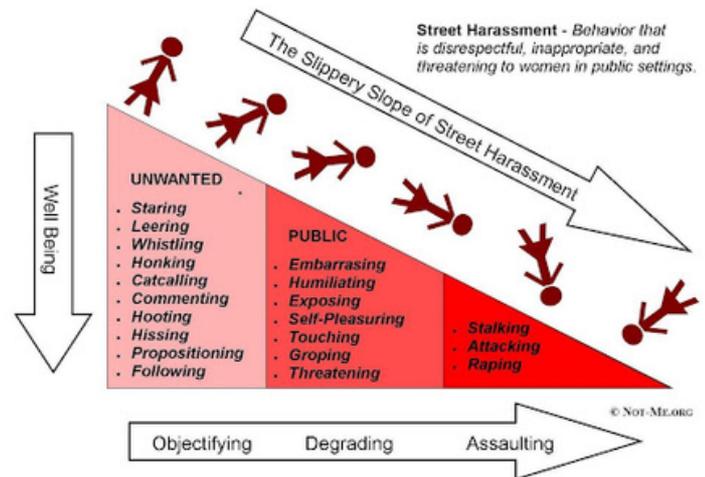
Young people often face the worst of this harassment—whether it be kids or young adults.

Did you know?

Oftentimes virtual harassment is dismissed as not being equivalent to offline harassment, however, the effects of it are too real to be ignored. People who face digital harassment are susceptible to long term psychological, emotional, and mental issues, such as depression, anxiety, isolation, and several others. In the United States alone, nearly 60% of teenagers have been bullied or abused online and children who face harassment are twice as likely to commit self-harm.



The Street Harassment Slippery Slope



Even though this graphic shows the consequences of street harassment, it can also be applied to online harassment. In such a connected world, it is becoming harder to point out the differences between physical public spaces and those spaces online. Online harassment is unwanted and public, and it objectifies, degrades and assaults its victims.

In online spaces the first section of “Unwanted” engagement can be seen in unwanted direct messages on gaming and social media platforms as well as unwanted comments in publications. The second set of examples shows that these forms of harassment are degrading and public. For instance, online the perpetrator interacts with victims through unsolicited pictures, messages, and sexual invites, for example. The last section is harder to identify in online spaces, but while online the assaultant can bribe victims to send pornographic images, as well as impersonate others online.

Online Child Abuse

As mentioned before, gaming is one of the most popular activities among young adults. Multiple consoles exist for consumers. However, the concentrated number of children and young adults on these platforms opens up space for youth to be exposed to pedophiles. The true magnitude of sexual abuse towards children is much higher than we think. **30% of children around the globe who are sexually abused online are in the United States alone.**

Keep an eye out!

Free online chat rooms, social networking sites, instant messaging apps, and discussion forums can serve as the perfect place for predators to find children to abuse. Often predators will start simple conversations with children to build trust, groom them, and then coerce them into performing sexual favours. Children between the ages of eleven to thirteen are most likely to be preyed upon, and a majority of child sexual imagery depicts female children.

Digital abuse of children includes, but is not limited to cyber bullying, grooming via chat, sexual abuse, circulating child porn, or coercion into performing sexual favours. During the pandemic, there was a spike in online child abuse, mainly self-generated, which is when abusers coerce children to create and upload sexual content from their own homes via webcams on laptops and desktops. In 2021, the amount of coerced child pornographic content grew online by almost 400%. Children are being groomed and forced to take part in their own abuse, in their own homes, unknown to parents and teachers.

How to Approach When a Child Reports Being Abused Online

It is extremely important to talk to children about online safety and educate them about using the Internet with caution. Teachers and parents can both inform children about potential risks online, how to combat predators, and how to browse the Internet safely.

Cyberbullying

Cyberbullying, another form of abuse that children are subjected to, often by people they know in real life. Being publicly humiliated online by peers, spreading rumors or having embarrassing media circulated, or being catfished and threatened via messaging are ways children can be cyberbullied. The anonymity and accessibility provided by the Internet makes cyberbullying and cyberstalking especially rampant.

But, there are ways to fight it. Fostering and encouraging positive interactions between children, campaigning against bullying, and conducting anti-bullying programs in schools are all ways that can reduce bullying, both online and otherwise.

Did you know?

More than 90% of American teenagers believe cyberbullying is a significant problem for their peers. 1 in 5 children in the USA experience severe mental health concerns as a result of bullying, and bullied children are likelier to develop suicidal thoughts. These numbers are higher for children who identify as LGBTQ, or those from marginalized backgrounds.

Keep an eye out!

Some common signs that may indicate that a child is being abused include:

- Isolating themselves;
- Seeming anxious, upset or distant;
- Being secretive of online activities;
- Sexualised behavior, using inappropriate language.

Any of these signs, when identified, need to be addressed immediately. Online abuse issues can be escalated to the relevant authorities. The National Society for Prevention of Cruelty to Children in the UK has helplines for children as well as adults. In the USA and Canada, the Childhelp National Child Abuse hotline is available for calls 24/7.

Online Harassment in Gaming, Virtual Reality, & the Metaverse

Child abuse, cyberbullying and online harassment have been further exacerbated with the invention of VR or Virtual Reality. Virtual Reality games completely revolutionized how consumers engage with video games. Users can now experience their games as if they are in those realities themselves.

Regrettably, there have been several reports of molestation, sexual harassment, stalking, and abuse occurring in virtual reality games.

While the invention of VR may have taken the gaming world by storm, the social spaces provided by it are still burdened with the problems of its predecessors. Chats are largely unmoderated, offering users an incredible amount of anonymity and access, which leads to multiple opportunities for predatory behavior.

RecRoom, a VR space for children, has a setting for children younger than 12 to sign up for a junior account, which comes with content blockers to shield the child from abuse. However, children often lie about their age during sign-up so that they are able to access the voice chat, texting, or event and club features.

This problem has permeated into the Metaverse as well. Since the metaverse is a mixture of Virtual Reality, Augmented Reality and Artificial Intelligence, users are able to create complex avatars, which are able to walk around in a completely virtual world. However, when Horizon Worlds, Metaverse's social media platform was opened up to users, there were complaints of inappropriate behavior and groping of avatars. The reactions to this news were largely dismissive, with most users saying that this could be avoided by simply logging off. However, this is reminiscent of victim blaming and begs the question, why should the ones who are being harassed be forced to leave and exit, rather than the harassers?



Censorship Vs. Safety



Peter

I see my kids talking about VR and Metaverse, and these spaces seems very dynamic, and I find it hard to introduce methods in my home to keep them safe. Sometimes I wonder if it would be best if I just took their devices away. Mr. Dan, what do you think I should do?

This is so hard! I've seen a lot of parents decide to reduce or completely remove their children's screen time, but that just makes them even more curious to be online whenever their folks aren't around.



Mr. Dan



Peter

What should I do then? I am so scared something will happen to them. The internet is so unsafe.

Sorry, I couldn't help but overhear the conversation! I think Peter, that we are currently raising children in an era in which there are not strong lines regarding age-appropriate content especially in gaming, so even if we try to limit their access to certain types of content, they will have access to it when they play with friends. As an example, I did not want my son, Pietro, playing Grand Theft Auto, which can be very violent, but one of his friends has an older brother, so they were playing it by the time they were nine or ten. Of course, I could prohibit him from going to any peers' homes, but it wouldn't work. What I did in my home, was I had a conversation with them about violence, and let him take his own conclusions. It went so well! Of course, you should approach it the way your kids will understand better, but censoring just to "protect" our kids might not be the best option.



Julia



Peter

That sounds like a great idea Julie! And thank you too Mr. Dan. Now I see that censoring them won't make them safer, it will just make them want to use it more. I will talk to them, maybe what I can do is talk to them about age restrictions, and maybe even convince them to take more extracurricular activities so they would spend less time in front of the screen!

PARENT-TO-PARENT/ TEACHER ADVICE



Mr. Dan

You know, I've been following this matter of online safety for a while now, and I am always impressed to see that some tech-savvy kids are taking their safety into their own hands.

I agree, the other day, my oldest son, Andre was talking to his brothers that he and his friends started to notice that sometimes, weird messages show up to them. He said "they were sending him messages that didn't sound like someone his age", and saying words like "honey", "darling". My whole body froze when he said that, but then, he said that him and his friends created some sort of code that directs the groomer into a virus, which will block their IP address from ever creating another account in that game!



Peter



Mr. Dan

Wow! That is incredible! You know, hacking has a negative reputation, but most hackers are what are called "white hat" hackers. These are individuals that hack and test for weaknesses in firewall defenses (electronic walls around things like banks or other secure silos of information) so as to anticipate issues before the bad hackers infiltrate. And it is an incredible skill that your son and his friends are picking up!

We should be engaging and mentoring these kids, directing their talents, rather than try to contain them or shut them down.

What was fascinating to me is that the more tech savvy kids are themselves gathering together in online spaces such as gaming platforms such as Roblox to look out for one another, and that happens globally! Kids are no longer contained in our homes. They are "free range" on a whole new level. But why are children having to do this? I think that our task as educators and parents is to learn as much as we can, and also get familiar with the laws in place, to protect our children.



Peter



Mr. Dan

Absolutely, Peter, but we also need to empower kids to be safety savvy so that they can protect themselves. So many times we are not around to see and protect. It is good that they know how to defend themselves too!

REPORTING ON SAFECITY

Whenever you see something, whether with you or with children around you, you can report it on SafeCity. Safecity empowers individuals, communities, police and city government to create safer public and private spaces.

To report on Safecity, you need to follow three simple steps:

1

Download the Safecity app on your phone or open the website on your computer.

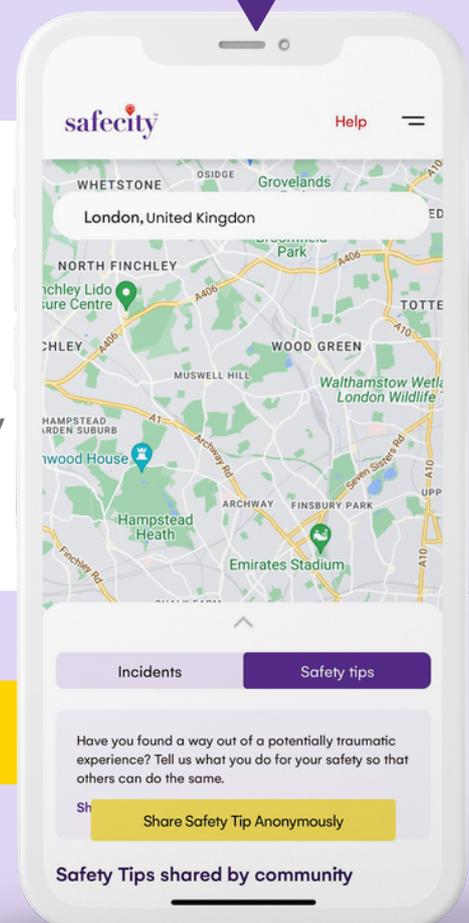
2

Fill out all the information requested about the situation you'd like to report.

3

If you'd like, answer a few more questions about the incident, which will help us map the types of violence better, and prevent future incidents from happening to others.

[Click here to download the app](#)



TAKING ACTION TO STOP ONLINE ABUSE AND HARASSMENT

Now that you have learned all these things about online safety, we gathered some of the do's and don'ts of internet safety to prevent and tackle online abuse and harassment!

DO'S

- Use a good antivirus software to keep your device free of malware;
- Use strong passwords and use two-step verification where possible;
- Look for the gray lock icon in the address bar of the Chrome browser to verify that the URLs are secure;
- Be mindful about what you post on social media;
- Use parental controls and app lock on shared devices;
- Educate children about using the Internet responsibly, ensure open communications and explain to them why internet safety is so important;
- Use a safe password manager instead of choosing 'remember password' on websites;
- Only input financial information on secure, trustworthy websites.

DONT'S



- Don't click on dubious links or 'too good to be true' reward websites;
- Don't give out your passwords or sensitive information on public computers;
- Don't give children unrestricted Internet access;
- Don't surf the Internet without using a VPN or virtual private network;
- Don't download random programs from the Internet;
- Don't install suspicious extensions on your browser;
- Don't respond to 'creepy' or suggestive messages.

SUPPORT US!

All of our work is non-profit. We believe that our work through Red Dot Foundation can help thousands of people all over the world with our solution. If you want to help us creating and sharing knowledge, feel free to donate to our institution.

Donate now!



Red Dot Foundation Global (USA)

[Paypal](#)

[Global Giving](#)

[Act Blue](#)

Find us on Benevity
and Amazon Smile

Red Dot Foundation India

[Donate](#)

Find us on Benevity

THANK YOU

for taking the time to prioritize online safety for the children in your life. Please refer back to this guide as much as needed, and reach out with any suggestions or questions at:

contact@reddotfoundation.org

