International Journal of Education and Social Science; Vol. 10 No. 3; December 2023
ISSN 2410-5171 (Online), 2415-1246 (Print)
Published by Research Institute for Progression of Knowledge

Cyberthreats: An Epidemic

Dr. Charles E. Notar (Emeritus)
Jacksonville State University
USA

Hudson T. Agee
Hoover High School
USA

Abstract

It is true to say that we live in a fast-paced, high tech, multi-media world these days. While it has many advantages, it has its dark side just as the physical world. Has technology been used to steal from you, bully you, stop you from advancement in your job or being accepted into a college? Cyberbullying is of major concern everywhere be it in the home, at school, or the workplace. This article presents the five most important things to do to prevent cyberbullying. What can be done about cyberthreats in the home, as a parent, as a child, and in school/workplace are discussed. The authors understand there are a myriad of articles that provide preventions but consider the following as the foundation for prevention: Communication and trust, education, teaching, privacy, and help.

Descriptors: Bullying, computer security, cyberbullying, cyberbullying, security, workplace bullying

Introduction

Cyberbullying

Bullying is deeply ingrained in American culture. Our society illustrates the pinnacle of capitalistic competition. This win-or-die-trying atmosphere, the competitive college acceptance process, and much of the corporate world, contribute to many of the bullying problems that we battle today. The issues of bullying and cyberbullying can only be contained in the short term and not eliminated entirely due to how deep-seated it has become in our competitive society (Donegan, 2012).

Because their motives differ, the solutions and responses to each type of cyberthreat and cyberbullying incident must also differ. Unfortunately, there is no "one size fits all" when cyberbullying is concerned. Only two of the types of cyberbullies have something in common with the traditional schoolyard bully. Experts who understand schoolyard bullying often misunderstand cyberbullying, thinking it is just another method of bullying. But the motives and the nature of cybercommunications, as well as the demographic and profile of a cyberbully differ from their offline counterpart (Sequoia Alternative Program, 2023).

Bullying has everything to do with the character of the aggressor and nothing to do with your child (Whitson, 2014). The goal of what you do as a parent is to protect and restore your child's self-respect when needed.

Governments and policymakers have a key responsibility to protect all children from bullying, including cyberbullying. Additionally, other stakeholders can play a significant role in protecting children from bullying. Parents and children play a vital role, as do other professionals - such as teachers and social workers, law enforcement agencies and the private sector. Media, too, has a vital role to play, as recognized, in part, by the World Health Organization's release of a resource for media professionals on preventing suicide, which highlights the importance of avoiding, "undue repetition of stories about suicide". All these stakeholders have a role in creating a safe environment that allows children and young people to benefit from the use of modern technologies without experiencing harm.

Cyberbullying consequences can be physical, emotional, and educational. Unlike normal bullying cyberbullying is often anonymous and can take place anywhere. This is a problem for everyone: parents, children, schools, law enforcement. Has technology been used to steal from you, bully you, stop you from advancement in your job or acceptance into a college? The range of cybercrimes from stealing, bullying, advancement in your job or acceptance into college will tempt you to stop using the internet entirely (Norton, 2020).

The exact reason of why people do cyber bullying is unknown. Revenge motivated some individuals to do cyber bullying. Being victims of bullying in daily lives make them think harassing other people is only something that is natural as some people deserve to be bullied (Gabriel, 2023). Cyberbullies can be anyone … it does not require a person to be face to face as seen in "normal" bullying, the cloak of anonymity provides the cyberbullies their strength.

The following are a few distinct behaviors associated with cyberbullying:

Offensive name-calling
Spreading of false rumors about them
Receiving unasked for explicit images
Posting fake information or obscene pictures of someone on social media
Sending abusive or threatening messages through messaging platforms
Pretending to be another person and sending obscene messages on their behalf.
Physical threats
Constantly being asked where they are, what they're doing, or who they're with by someone other than a parent
Having explicit images of them shared without their consent
Deepfakes of videos, voices, and pictures

Cyberthreats infringes on your right to human dignity, privacy, freedom, and security. Research has shown that cyberbullying can adversely affect a person's mental health. Cyberbullying can lead to anxiety, depression, social isolation, emotional distress, low self-esteem, and academic difficulties. Psychological stress worsens with repeated abuse (Celik, et al., 2012; GITNUX, 2023; Kolonko, 2022).

Numbers {Sample of statistics on cyberbullying]

More than 97% of youths in the United States are connected to the Internet in some way (Tokunaga, 2010). Ninety-five percent of teens now report they have a smartphone or access to one. These mobile connections are in turn fueling more-persistent online activities: 45% of teens now say they are online on a near-constant basis (Anderson, & Jiang, 2018).

A survey of 1,316 teenagers aged 13-17 in the US reveals that 97% now use the internet every day, up from 92% in 2014-15. However, the Pew Research Center's most striking finding is perhaps that 46% say they use the internet "almost constantly" – a significant rise from 24% in 2014-15 (Ellerbeck, 2022).

Twenty-one percent of children have been cyberbullied (Security, 2023). Of all the social networks, kids on YouTube are the most likely to be cyberbullied at 79%, followed by Snapchat at 69%, TikTok at 64%, and Facebook at 49% (Security, 2023).

As a child's age increased, so did the likelihood of cyberbullying. As the child aged in two-year intervals between the ages of 10 and 18, their likelihood of being cyberbullied increased by two percent (Security, 2023).

About 80% of youth believe cyberbullying is easier to get away with than in-person bullying (GITNUX, 2023). As you can see from the numbers above kids are wide open to cyberbullying. The numbers demonstrate the serious of cyberbullying and why there is a need for awareness of its effects so all parties can work together towards finding solutions (GITNUX, 2023).

Prevention

Cyberthreats are everyone's business and the best response is a pro-active preventative one. The focus on "prevention" recognizes that change is ultimately about shifting behaviors and attitudes, which can happen through the positive approach of education, awareness, and action (National Centre Against Bullying, 2023). It's a good idea to know how to recognize cyberthreats. The first step to helping protect yourself and your data is taking some basic precautions and knowing who to contact when you see others engaged in offensive online activities [criminal, personnel] (Norton, 2020).

There are multiple players and locations involved in the prevention of cyberthreats. Cyberthreats are of major concern everywhere be it in the home, at school, or the workplace. In fact, no one and no place is safe from the insidious fast-paced, high tech, multi-media world. Besides the individual who poses the threat there are parents, schools, media companies, and bystanders. As the key in cyberthreats the authors did not want YOU to be lost in the list of players in the prevention of cyberthreats. Where do we start to prevent cyberthreats? The authors decided to start with the home.

A man's home is his castle. A man's home is his castle is a proverbial expression that illustrates the principle of individual privacy. Cyberthreats are everyone's business and the best response is pro-active preventative one. Prevention requires a change in behaviors and attitudes through education, awareness, and action **(**Norton, 2019).

Parents

A man's home is his castle. It is your primary responsibility to protect that which is yours regardless of the threat. You as parents give your children lessons and rules to stay safe in the real world – look both ways before crossing the street, don't talk to strangers, always wear a helmet.

Yet when it comes to the online world, many parents are putting their child behind the wheel of a car without instruction or supervision. It's no surprise that many children and even adults are unprepared to deal with the realities of cyberbullying (Bauld, 2022).

Be A Parent and provide pro-active preventative instruction on cyberbullying.

Being a parent by far is the toughest job when dealing with cyberthreats, but it means understanding what's appropriate for your children, and understanding — even monitoring — what they're doing online. It means setting rules with consequences and sticking to them and taking care to make sure your children understand what it means to be safe on the internet (Notenboom, n.d.). The authors of this article firmly put the onerous on the parent on providing pro-active preventative instruction on cyberthreat and particularly cyberbullying. Why because the parents are providing the internet, phone, and other vehicles for the child.

YOU as a parent aspire for your child/children. For them you want a happy and safe childhood, good schooling, and great jobs in their future. A key ingredient in protection is teaching right and wrong. This is particularly true in the technology age we live in today.

Just as you protected your castle you must protect your loved ones. One of the many responsibilities of a parent is protection. You are the first line of defense because you are *the most important teachers.*

The authors believe there are five MUSTS that are the foundation of any prevention plan. First and foremost is communication and trust.

Communication and Trust

(Abramson, 2022; Clifford, 2012; National Centre Against Bullying, 2023; Norton, 2020; Notar, Beard, & Akpan, 2020; NYC Public Schools, 2023; Positive Action, 2023; Sequoia Alternative Program, 2023; TeachThought Staff, 2015; United Nations Development Programme, 2023; Whitson, 2014.

Communication

(Abramson, 2022; Norton, 2020; Notar, Beard, & Akpan, 2020; stopbullying, 2023).

Communicate. Talk! Listen! Talk to your children about the internet. Reduce the risks associated with Internet use by engaging in an open discussion with your children about their online activities. Understanding and learning about your child's situation will not only help solve the problem but will also allow your child to be more open. Abramson (2022) states communicating regularly about cyberbullying is a critical component in preventing it from affecting your child's well-being. You can instruct your kids about acceptable use of the internet without shutting down communication channels. Make sure they know that they can come to you if they're experiencing any online harassment, stalking, or cyber incivility (Norton, 2020; Notar, Beard, & Akpan, 2020).

Communication and trust are first and foremost in combatting cyber bullying. They are in all relationships. You can reduce the risks associated with your children if you engage in an open discussion with our family about their online activities and set up rules that will grow along with them. Cyberthreats are of major concern everywhere be it in the home, at school, or the workplace. In fact, no one and no place is safe from the insidious fast-paced, high tech, multi-media world. Being a parent by far is the toughest job when dealing with cyberthreats, but it means understanding what's appropriate for your children, and understanding — perhaps even monitoring — what they're doing online. It means setting rules with consequences and sticking to them and taking care to make sure your children understand what it means to be safe on the internet. The authors of this article firmly put the onerous on the parent on providing pro-active preventative instruction on cyberthreats and particularly cyberbullying. Why may you ask - it is simply - who provided the internet, phone, and other vehicles for the child?

You, as a parent have aspirations for your child/children. For them you want a happy and safe childhood, good schooling, and great jobs in their future. A key ingredient in protection is teaching right and wrong. This is particularly true in the technology age we live in today.

Just as you protected your castle you must protect your loved ones. One of the many responsibilities of a parent is protection. Parents are the most important teachers.

Talk! Listen! From the outset, we can reduce the risks associated with Internet use if we engage in an open discussion with our children about their online activities. More than 97% of youths in the United States are connected to the Internet in some way.

A key to developing communication is not overreacting or underreacting by blaming your children or telling them to "shrug it off" or just deal with the bullying. When your child is faced with cyberbullying you as the adult must act thoroughly; fast decisions can only make things worse. Talk to someone about the problem before responding. Collect evidence and join with teachers and others to figure out the possible best choice to stop cyberbullying among children (stopbullying, 2023).

Psychologists will tell you that the best way to help your child is to have a conversation first. Know what your child is doing online and with their cell phones and other devices. Supervise and increase effective monitoring of the internet. Get to know your children's friends, are they the type of kids that are positive influences (Abramson, 2022; Norton, 2020; Notar, Beard, & Akpan, 2020; stopbullying, 2023).

Trust

(ConnectSafely, 2020; Coopwer, 2021; 2023; Hirsh, 2023; National Centre Against Bullying, 2023; Parents editors, 2019; Positive Action, 2023; Safe Search Kids, 2023).

Remember if your child is on the receiving end of cyberbullying it is not their fault and that they do not deserve to be viewed this way. Bullying has everything to do with the character of the aggressor and nothing to do with your child. This is a critical reminder for kids (Whitson, 2014).

Be there for your kids they must know that they can always come to you or another trusted adult if they are in trouble. Let your child know that you have their backs. Make sure your child feels safe. They must know that they can always come to you or another trusted adult if they are in trouble. Love them. Mentor them. Teach them. Remember if your children is on the receiving end of cyberbullying, remind them that it is not their fault and that they do not deserve to be treated this way. The goal of what you do as a parent is to protect, build and restore when needed your child's self-respect.

In summary, communicating regularly about cyberbullying is a critical component in preventing it from affecting your child's well-being. Establish a climate of communication with your child. Encourages communication by listening to your child. *Talk frequently and openly. Constantly support your child* by t*elling them you believe him/her and that you appreciate him/her sharing.*

A Word of CAUTION. The world is plugged in. Technology … iPhone, earbuds, headphones ... are ubiquitous. In the past decisions such when to start dating, when to wear makeup, when and how much should an allowance has been supplanted by when does the "kid' get the iPhone. Our education system in the United States has already determined when they get a computer … first grade.

Today's children identify closely to their online presence and interactions What happens online is profoundly serious to them, and they do not take it lightly. Their online persona is the same to them as their real person. If a child comes to you with a problem, don't try to minimize it. Address it immediately and find resources and make it obvious that you understand it is serious.

Keep in mind kids may be hesitant to open up about cyberbullying because they're afraid they'll lose access to their devices. Don't threaten to take away your children's phone or computer if they come to you with a problem. Build trust with your children. Encourage your child to be open with you by reminding them they won't get in trouble for talking to you about cyberbullying. Clearly explain your goal is to allow them to communicate with their friends safely online

Educate

(Abramson, 2022; AO Kaspersky LabTop, 2023; De Leach, 2023; Delete Cyberbullying, 2023; NYC Public Schools, 2023; Positive Action. 2023; Safe Search Kids, 2023; TeachThought Staff, 2015; United Nations Development Programme. 2023).

While the authors started with communication and trust education is the necessary foundation for these to be successful. Prepare them. Recognizing cyberthreats is the first step to helping protect your children from being compromised. Basic precautions and knowing who to contact when you see others engaged in offensive online activities [criminal, personnel] are part of this first step (Norton, 2020).

Basics of education include defining cyberbullying. Recognize the signs and symptoms such as increased device use, anger or anxiety after using a device, or hiding devices when others are nearby. Your communication and help will to an extent depend on your understanding cyberbullying's scope and its mental and physical ramifications. The authors suggestion you start your education with the Pacer National Bullying Prevention Center, 2023 and Stopbullying.gov 2021.

Teach Students to be Smart Online

(A Stop Online Harassment Project, n.d ; Ahmed, 2017; Beard, Akpan & Notar, 2020; ConnectSafely, 2020; Coopwer, 2021; De Leach, 2023; Delete Cyberbullying, 2023; 2023; Facebook, n.d.; Gordon, 2022; Hirsh, 2023; ICDL Arabia, 2016; Kiplinger, 2023; National Centre Against Bullying, 2023; Makad, 2018; MediaSmarts, n.d.; Nelson, 2023; Net Nanny, 2016; Norton, 2020; NYC Public Schools, 2023; Pavlovic, 2023; Positive Action, 2023; Schifferle, 2015; TeachThought Staff, 2015; Whitson, 2014).

Internet privacy is the privacy and security level of personal data published via the Internet. It is a broad term that refers to a variety of factors, techniques and technologies used to protect sensitive and private data, communications, and preferences.

Passwords

Passwords exist for a reason. They protect you. Therefore, Protect your passwords. Passwords MUST be private. Keep them to yourself. Don't share your passwords with anyone – even your closest friends, who may not be close forever. Keep your personal and private information locked down (Norton, 2020).

It may be tempting to use the same username and password wherever you can to make things simple. If you use the same username and password and your credentials are compromised or leaked someone would be able to access not just that site but other sites as well that you use.

A good password should be unique. Even though it may be tempting to use the same password for all your online accounts, which would not be a wise decision. If someone was able to discover your password, they would have access to all your accounts. You should create a unique password for each account. Make sure you have passwords on your phone, computer, and all online accounts. Use strong passwords and change them regularly. Having multiple emails for different categories or activities can also be a tool not only for the organization but also for online security.

For a strong password a rule of thumb **is** use at least 8 characters to include at least one number, one capital letter and one symbol. This rule has been extended due to the abilities of computer programs and hackers to crack passwords. Create a long password of 12 characters or more. Each additional symbol in a password exponentially increases the number of possible combinations.

While creating a strong password there are things you should NOT use:

something generic. Ex. "password", "12345" etc.
memorable keyboard strokes Ex. "qwerty", these passwords are very easy to crack.
personal information. Ex. nickname, date of birth, pet's name etc.
recycled passwords. Ex. Used last year; used on another device.

Password Management

While working on many different applications online you may need to keep track of usernames, email addresses, and passwords. Trying to keep track of many different credentials may become very overwhelming. It is recommended to use a password manager in this case (NYC Public Schools, 2023).

Other Methods of Securing Your Devices

Passphrase

Use a passphrase rather than a password. Passphrases are much more secure than passwords because they are typically longer, making them more difficult to guess or brute force. So instead of choosing a word, pick a phrase and take the first letters, numbers, and punctuation from that phrase to generate a seemingly random combination of characters. You can even substitute the first letter of a word with a number or symbol to make it even more secure.

Dictionary

Another method for choosing a password is to open a dictionary or book and choose a random word. But as a random, as it may seem to you, a single word is quite easy for a hacker to guess. So rather than opting for just one word from the dictionary, choose a few and string them together along with numbers and symbols to make it much trickier for someone to figure out.

Using two-factor authentication

The idea behind two-factor authentication is to use two factors (things) to authenticate your credentials when logging into an online application or site. Even if someone does manage to steal your password, you can still prevent them from accessing your account by adding an additional layer of security with two-factor authentication.

Enable two-step verification on your apps. Given the weakness of passwords in the unique identification system, more services are using two-step verification. The two-step verification is to use the second code to identify unknown computers. This code is normally sent to the mobile phone. So, if a stalker has your password, he will not be able to enter your account.

Anyone trying to log in to your account will have to enter the second piece of information after the correct password [Ex. Username + Code (Authenticator App)]. This is usually a one-time code that'll be sent directly to you via text message, although this isn't necessarily the most secure way of receiving that code.

It's much safer to use a two-factor authentication app instead, as they're much trickier to intercept. Below are a few authentication apps:

Google Authenticator
Microsoft Authenticator
Authy

VPN

A VPN — short for virtual private network. A VPN disguise your online identity by encrypting all traffic leaving your devices until it arrives at its destination. If cyberbullies do manage to hack your communication line, they won't intercept anything but encrypted data. VPNs also make it more difficult for third parties to track your online history, personal information, and data. It's a must to use a VPN when you use a public Wi-Fi network in a library, café, hotel, or airport.

Multi-factor authentication

Using a physical token (like a Yubikey) or a personal device (like a mobile phone) to authenticate users ensures that passwords are not the sole gate to access (onelogin, 2023).

Remote access

Using a smart remote access platform like OneLogin means that individual websites are no longer the source of user trust. Instead, OneLogin ensures that the user's identity is confirmed, then logs them in (onelogin, 2023).

Biometrics

A malicious actor will find it very difficult to replicate your fingerprint or facial shape. Enabling biometric authentication turns your password into only one of several points of trust that a hacker needs to overcome (onelogin, 2023).

Webcam Threats

While we are on insuring no one can get to our information there are multiple examples of malware designed to specifically target webcams to allow hackers secretly watch their victims. Most malware designed to hack webcams are usually accessed by getting victims to visit infected websites, opening malicious email attachments or by plugging USB drives into their PCs. Covering your webcam. Scan your computer for webcam malware. Additionally check to ensure that your webcam is secured, many webcams and even security camaras are unsecured and can easily be accessed, no hacking needed.

If you are using a standalone camera in conjunction with your computer, make sure you have changed the default settings that are configured by the manufacturer. Please read the instructions that came with your webcam to find out how to change these settings.

Internet security programs

.Internet security programs. To protect your home there are some basic precautions. Start with using full-service internet security suite [e.g., Norton Security, McAfee, Norton].

Go high tech and strengthen your home network (Norton, 2020; ICDL Arabia, 2016

Using privacy controls

In our communication about cyberthreat risks setting up online activities and rules that will grow along with them should be a major item of discussion. Talk to other parents and the school because they will have help hints and mor importantly you child will ”cite” what their friends can do or what the school has said in their defense. Based on age and maturity explain you will monitor computer activity. This will be a touchy subject. First you must be calm and reassuring. The discussion should include explaining age limits and age-appropriate sites. Talk about what is fake and what is real and agree to ground rules. Explain what online activities and behavior you are monitoring.

Investigate what measures you can take to keep content private on the websites you use. It is understood that each app, website, and device have unique privacy settings. On Facebook and other social networking sites, you can adjust your settings so that only the people you select are able to see your personal information and posts. It’s important to check these privacy settings frequently, because sites sometimes change their policies (A Stop Online Harassment Project, n.d.). Give them the empowering message that they oversee how they are treated by others. Encourage them to use privacy settings to set boundaries on cruelty by their peers (Whitson, 2014). Adjust your privacy settings and review them often (Facebook, n.d.).

Parental controls

Parental controls are software and tools that allow parents to set controls on their children's internet use. They are a great way of helping prevent children from accessing unsuitable content online (NYC Public Schools, 2023).

The talk of parent “controls” can sometimes be confusing. There are three types of controls parents need to be aware of:

- Network-level controls are set on the hub or router and apply to all devices connected to that hub or router (covering your whole household.)
- Device-level controls are set on devices, such as a smartphone, and will apply regardless of how and where it is connected to the internet.
- Application controls are set on the platform or application that is being used. Examples of this would be the settings applied to Google or YouTube. Check that they are working on each device your child accesses (NYC Public Schools, 2023).

Tools like parental controls can help protect your children from accessing inappropriate content, but you can’t check everything they see on the internet. You need to help them avoid unsuitable content, and cope with it if they see it. The first step is to talk to them about it. Below are a few tips on what conversations should be started with your children about what they see online.

Consider implementing parental controls - Most devices can be set up so you can not only actively see what your child is doing but also keep a log of everything your child has seen or accessed. You may be able to set some parental controls within your browser. For example, Internet Explorer allows you to restrict or allow certain websites to be viewed on your computer, and you can protect these settings with a password. To find those options, click Tools on your menu bar, select Internet Options, choose the Content tab, and click the Enable button under Content Advisor (NYC Public Schools, 2023).

Tech usage agreements/contracts.

In the first sentence of Using privacy controls, we used the term monitoring. You and your children set up rules of usage and supervision to include effective monitoring of the internet. Discuss consequences (losing their cell phone and/or computer privileges) associated with the rules. The rules must include how to report things that look suspicious. While establishing rules include teaching them to respect others and to take a stand against bullying of all kinds helps provides reasoning for rules. Regularly checking their device by hand or through other software can also assist in keeping the rules followed.

Set rules the rules explaining why, and the dangers associated with them. Ensure your child knows the boundaries of what they are allowed to do on the computer. They should be appropriate for the child's age, knowledge, and maturity. Set time limits, explain your reasons for them, and discuss rules for online safety and Internet use, what sites they are allowed to visit, what software programs they can use, and what tasks or activities they are allowed to do.

Ask your children to contribute to establishing the rules; then they'll be more inclined to follow them. Homes should create online agreements or contracts for computer use, with input from students or kids. Make sure your agreement contains clear rules about ethical online behavior. With younger children who visit games sites, rules should deal with online interactions: never provide personal information and don't share passwords with friends. For teenagers, social activity online is intense. This is the time to discuss the nature of your teen's online interactions and, more specifically, his or her responsible use of the Internet (MediaSmarts, n.d.). *At the end of the day, the most important thing is building trust with your child. Explain why online rules exist, remind them that you trust them, and encourage them to talk to you if anything goes wrong.*

Be SMART When Using Your Devices

Think before you post.

Never forget that the internet is public. What you put out there can never be erased. If you wouldn't say something in a room full of strangers, don't say it via internet. Even letting someone know sensitive or embarrassing information about you via email can have unforeseen consequences. Posting something embarrassing about yourself may come back to haunt you later in life, like when you're trying to get into a college or interviewing for a job. It has become common practice for professional organizations to comb through the social media profiles of potential candidates to determine what type of person they are. Don't give them a reason to judge and reject you. Remember this important tip - if you wouldn't want your mother to see it, don't post it. The moment you post an image or comment, that information can be copied and reposted thousands of times over, and you'll lose the chance to delete that information forever (Delete Cyberbullying, 2023; .Facebook, n.d.; Notenboom, n.d.; Twitter, n.d.).

Sharing Personal Information

DO NOT share your address, phone number, family members' names, car information, passwords, work history, credit status, social security numbers, birth date, school names, passport information, driver's license numbers, insurance policy numbers, loan numbers, credit/ debit card numbers, PIN numbers, and bank account information (A Stop Online Harassment Project, n.d.).

Keep your personal and private information locked down. Social engineering cybercriminals can often get your personal information with just a few data points, so the less you share publicly, the better (Norton, 2020).

Think before you post anything online or share information in emails. What you post online, can be seen by anyone. Sharing personal information with others you do not know personally is one of your biggest risks online.

Photos are a cyberbullies best friend. Those taken from smartphones embed the GPS Coordinates in the photo. Those pictures posted online may be copied, altered, and shared without your knowledge or consent, unless you use privacy settings to limit who has access to the pictures.

Helpful Think Smart Hints

Log off public/classroom computers and keep your phone locked in group settings
Don't be gullible
Beware of certain topics
Never open messages from strangers
Don't respond to an angry message with anger
Don't forward chain mails, hoaxes or long emails
Never open messages from people you don't know
Proofread your messages
Pause before you post

Think before posting an angry or hostile response. (AO Kaspersky. 2023; De Leach, 2023; Delete Cyberbullying, 2023; Gordon, 2022; LabTop, 2023; Positive Action, 2023). (). (De Leach, 2023).

Know What To do If You Become a Victim

Block bullies/Don't respond

Bullies get satisfaction when you react to their offenses. If you stop responding to harassment, a bully is likely to lose interest and leave you alone. Just try not to react and immediately inform a family member about it.

Effectively dealing with cyberbullying.

Whether you are a kid or adult do not react to an online bully. Don't fight back. A lot of times bullies are looking to get a rise out of the those they are targeting. Fighting back just gives them what they want. The following are some basic guidelines:

Do not Reply to messages that harass or annoy you. Even though you may really want to, this is exactly what the sender wants. They want to know that they have got you worried and upset. They are trying to mess with your head, do not give them that pleasure.

Your response has upped the ante on aggression and the person who "started" it will escalate their cruelty even farther.

Your response creates equal culpability in the eyes of adults. Accountability is not based on "who started it?" but rather, who did the right thing to bring the situation to an end? It can potentially land both kids in legal jeopardy, since cyberbullying can be a criminal offense

A young person's instinct in a cyberbullying incident may be to retaliate -- to return the insults, post equally lewd photos or spread vengeful rumors. Teach them never to give in to this temptation.

If you respond with an even nastier message, it makes them, think that they really got to you, and that's just what they want. They might even complain about you!

Installing an app to block calls and SMS On Android and iPhone, can assist you with distancing yourself from the cyberbully. You'll find apps that can create call blocking lists and messages. They are particularly useful for blocking stalkers over the phone when the operator does not want or cannot lock a phone number. On Android, you have Blacklist Plus, while the new phones can block contacts without the need for an additional application (Ahmed, 2017).

Use available tech tools.

Most social media apps and services allow you to block the person. You can also report the problem to the service. That probably won't end it, but you don't need the harassment in your face, and you'll be less tempted to respond. If you're getting threats of physical harm, you should call your local police (with a parent or guardian's help) and consider reporting it to school authorities (ConnectSafely, 2018; Beard, Akpan & Notar, 2020).

Most social networks have mechanisms to block certain users (Facebook and Twitter have for example). E-mails can be filtered using automatic rules, and most e-mail applications create a list of contacts to block. On personal sites, temporarily disable comments and forms: it's a strategic retreat that will give you the peace of mind you need to take action (Ahmed, 2017).

Protect your PC from intrusion

One of the goals of the cyberstalker is to get information about you. In the worst case, this can happen through unauthorized access to your PC or phone. Learn how to block your PC and detect unauthorized access signs. If you do not feel qualified enough, ask a forensic computer expert for help – this is the best way to avoid hasty conclusions that could make the problem worse (Ahmed, 2017).

Pure and simply advice when cyberbullied …do not respond or retaliate. Secondly, BLOCK the bully on all online platforms. Most devices have settings that let you electronically block emails, messages, or texts from specific people (Ahmed, 2017; Child Mind Institute,.2023;ConnectSafely, 2020; 2023; Frejd, 2023; Gordon, 2022; Hirsh, 2023; Nelson, 2023; Parents editors, 2019;.Pavlovic, 2023; Webwise, n.d ; Whitson, 2014).

Next, document and report the cyberbullying. Save and make copies of all contact with the bully. Keep photos, screenshot s,and print out all the messages as proof and evidence of cyberbullying (AO Kaspersky 2023; Child Mind Institute,.2023; ConnectSafely, 2020; Frejd, 2023; Gordon, 2022; LabTop, 2023); Parents editors, 2019; Pavlovic, 2023; Safe Search Kids, 2023).

Get Help

Report cyberbullying. ***Tell someone you trust. Notify the Authorities.*** Most young people don't tell their parents about bullying online or offline. So, if your child's losing sleep or doesn't want to go to school or seems agitated when on their computer or phone, ask why as calmly and open-heartedly as possible. Feel free to ask if it has anything to do with mean behavior or social issues. However, even if it does, don't assume it's bullying. You won't know until you get the full story, starting with your child's perspective.

Remember **Communication and Trust**. Talking to your parents, friends, or someone you trust is usually the first step in dealing with any issue. In the case of school related bullying messages, you should also talk to a teacher you trust or guidance counsellor (28). Too often, young people get the message that they should be strong enough to handle problems such as bullying on their own. Help kids understand that reaching out to trustworthy adults is an act of tremendous strength and courage. Make sure your child knows that he never has to "go it alone." Rather, adults can do a lot to make cyberbullying situations better -- but they can't do anything if they do not know about them, so kids must find the courage to reach out and speak up (Whitson, 2014; Webwise, n.d.).

If you fear for your safety, notify the authorities If you fear for your physical integrity, contact the authorities. But do it in a calm and measured way (do not show up at a police station at four in the morning, they might think you're crazy!). They will collect data on harassment and the harasser, such as the IP address of their e-mails. Try to bring a friend or family member with you

Report offending content to administrators. Most services offer options to inform administrators of inappropriate or offensive content. This can not only constitute additional evidence but also allows the definitive expulsion of the harasser of certain services. There are instructions on Facebook, Twitter, Gmail, and others. Do a search on the official help and on the support page (Ahmed, 2017).

Report the bully to your service providers and social media sites. Block the harasser or restrict access to your person. Most social networks have mechanisms to block certain users (Facebook and Twitter have for example). E-mails can be filtered using automatic rules, and most e-mail applications create a list of contacts to block. On personal sites, temporarily disable comments and forms: it's a strategic retreat that will give you the peace of mind you need to take action (Ahmed, 2017).

Your report may assist authorities in their investigations or may help to thwart cyberbully from taking advantage of other people in the future. In some cases, cyberbullying may be classified as a crime, which places it beyond the jurisdiction of schools and service providers. If the cyberbullying involves one of the following elements, call your local police department, or report to the officer stationed at your school.

- Threats of violence or death.
- Sexually explicit photos or descriptions of sex acts. If the images are of a minor, this may be considered child pornography.
- Secretly recorded photos or videos that were taken without the subject's knowledge.

Hateful texts or online messages that single out and harass the victim based on certain features, such as race, gender, religion, or sexual identity.

(Ahmed, 2017; AO Kaspersky. 2023; Child Mind Institute,.2023; (ConnectSafely, 2020; De Leach, 20232023; Frejd, 2023; Gordon, 2022; Hirsh, 2023; LabTop, 2023; Nelson, 2023; NYC Public Schools, 2023; Parents editors, 2019; Pavlovic, 2023; Safe Search Kids, 2023; TeachThought Staff, 2015; Whitson, 2014).

Some instances of cyberbullying may be determined by law enforcement or schools to require you to consult with a legal expert (Safe Search Kids, 2023).

School

Report offending content to school administrators. Tell a person in authority what's going on, and explain to them the ways in which you're being cyberbullied. If you're not comfortable talking to a principal, talk to your favorite teacher or the school counselor. Every school has a policy for dealing with bullying, and more and more schools have a specific plan for putting a stop to cyberbullying.

- No matter what your school's individual policy might be, it's part of the administrators' job to resolve the situation.
- If you're a child or teenager, know that taking this issue to the school is the right thing to do. Other kids at the school may be experiencing cyberbullying, too. The school needs to be made aware of the problem to take steps to end it.
- If you're a parent, set up a meeting with the school principal to address the problem head-on.

Your school should have a cyberbullying policy. In fact, there should be a zero-tolerance policy for all types of bullying. If not, advocate for a strong policy. Get parents involved (Ahmed, 2017; Coopwer, 2021; Parents editors, 2019; Positive Action. 2023; Safe Search Kids, 2023; United Nations Development Programme. 2023).

Discussion

Anything we do to stop cyberbullying should be proactive. However, we are reactive. With the advances in technology and the joy individual have on beating systems cyberbullying will be difficult to contain, let alone stop. Recent articles on doorbell cameras and game apps being used to cyberbully are excellent examples of what lies ahead.

As a child, teen, young adult, or adult you want your online experience to be as safe as possible. Always be mindful that your personal security should always be your number one priority. Unfortunately, cyber threats will always exist and will continue to evolve and adapt to new technology. Consequently, we must also evolve and adapt to new technology and challenges. If you're a victim of cyberthreats and you feel helpless, know that you have the power to put an end to them. By following the tips in this article, you should be able to solve any difficult situation that may arise during your online experience. Of course, if they persist despite your best efforts, inform a parent, teacher, or proper authority right away. Always be aware of who you're talking to and stay safe.

Learn the technology. You don't have to know how a car's engine works to drive safely, but you do have to know how to drive and the rules of the road. The same is true for the internet. Take the time to learn about your computer, the internet, and the sites and services that you use most often. It's simple: the better educated you are about these things, the safer you'll know to be (Notenboom, n.d.).

Conclusion

Cyberbullying is well-recognized as a severe public health issue which affects both adolescents and children (Zhu,, et al., 2021). As more is learned about the reasons behind cyberthreats/bullying and the specific tactics utilized, prevention programs are becoming increasingly more effective. The biggest struggle for cyberbullying prevention in the future is matching the fast pace of technological innovation with effective preventatives requiring further development and exploration (Donegan, 2012); Zhu, eta l., 2021).

References

Abramson, A. (2022, September 7). *Cyberbullying: What is it and how can you stop it?* Retrieved from https://www.apa.org/topics/bullying/cyberbullying-online-social-media

Anderson, M, & Jiang, J. (2018, May 31). *Teens, social media and technology 2018.* Retrieved from https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018/

AO Kaspersky LabTop (2023). *10 Ways to stop cyberbullying*. Retrieved from https://usa.kaspersky.com/resource-center/preemptive-safety/top-10-ways-to-stop-cyberbullying

A Stop Online Harassment Project. (n.d.). *Delete cyberbullying: What can you do to help prevent cyberbullying?* Retrieved from http://endcyberbullying.net/preventing-cyberbullying/

Ahmed, R. (2017). *Cyberbullying: 10 Tips to protect yourself against cyberbullying.* Retrieved from https://www.hayzedmagazine.com/cyberbullying/

Bauld, A. (2022, July 8). *What to know about cyberbullying.* Retrieved from https://www.usnews.com/education/k12/articles/what-to-know-about-cyberbullying

Beard, L. A., Akpan, J., & Notar, C. E. (2020). Cyberincivility in higher education. *International Journal of Arts, Humanities and Social Studies (IJAHSS), 2*(4), 24-30. https://ijahss.in/Archive/vol-2issue-4/24-30.pdf

Bosco Legal Services, Inc. (2023, January 16). *How to stop online harassment: Laws, reporting, & what you can do*. Retrieved from https://www.boscolegal.org/blog/how-to-stop-online-harassment/#:~:text=Block%2C%20Mute%2C%20Report,with%20you%20in%20any%20way.

Celik, S., Atak, H., & Erguzen, A. (2012). The effect of personality on cyberbullying among university students in Turkey. *Egitim Arastirmalari - Eurasian Journal of Educational Research, 49*, 129-150

Child Mind Institute. (2023). *How to help kids deal with cyberbullying.* Retrieved (2023, May 2) from https://childmind.org/article/help-kids-deal-cyberbullying

Clifford, M. (2012, October 26). *15 Strategies educators can use to stop cyberbullying*. Retrieved from https://www.opencolleges.edu.au/informed/features/15-strategies-educators-can-use-to-stop-cyberbullying/

ConnectSafely. (2018). *Tips to help stop cyberbullying.* Retrieved from http://www.connectsafely.org/tips-to-help-stop-cyberbullying/

Coopwer, J. (2021, February 10). *Cyberbullying at school: 5 simple steps to protect students.* Retrieved from https://www.schoolnow.com/blog/cyberbullying-at-school-5-simple-steps-to-protect-students

De Leach, B. (2023). *10 Tips for teens to prevent cyberbullying.* Retrieved (2023, May 3) from https://www.momsteam.com/health-safety/10-tips-teens-prevent-cyberbullying

Delete Cyberbullying. (2023). *Deleting cyberbullying*. Retrieved (2023, May 4) from https://www.endcyberbullying.net/preventing-cyberbullying

Donegan, R. (2012). *Bullying and cyberbullying: History, statistics, law, prevention, and analysis.* Retrieved from file:///C:/Users/Charles%20Notar/AppData/Local/Microsoft/Windows/INetCache/IE/KNM25PCC/04DoneganEJSpring12%20(1).pdf

EBen-Joseph, E. P. (2023). *Cyberbullying.* Retrieved from (2023, May 3) https://kidshealth.org/en/parents/cyberbullying.html

Ellerbeck, S. (2022, Aug 30). *Half of US teens use the internet "almost constantly". But where are they spending their time online?* Retrieved from https://www.weforum.org/agenda/2022/08/social-media-internet-online-teenagers-screens-us/

Facebook (n. d.). *How can I stay safe on Facebook and what safety resources are available to me?* Retrieved from https://www.facebook.com/help/122006714548814?helpref=popular_topics

Frejd, S. H. (2023). *5 Ways to stop cyberbullying*. Retrieved (2023, May 8) from https://justbetweenus.org/everyday-life/christianity-and-culture/5-ways-to-stop-cyberbullying/

Gabriel, G. (2023). *What are the causes of cyber bullying?* Retrieved (2023, April 14) from https://english.binus.ac.id/2015/06/22/what-are-the-causes-of-cyber-bullying/#:~:text=The%20exact%20reason%20of%20why,people%20deserve%20to%20be%20bullied.

Geada, N., & Anunciacao, P. (2021). Reviving businesses with new organizational change management strategies. IGI Global.

GITNUX Newsletter. (2023, March 24). *The most surprising cyberbullying statistics and trends in 2023*. Retrieved from https://blog.gitnux.com/cyberbullying-statistics/

Gordon, S. (2020, July 10). *8 Motives behind why kids cyberbully*. Retrieved from https://www.verywellfamily.com/reasons-why-kids-cyberbully-others-460553

Green, P. (n. d.). *7 Ways to prevent cyberbullying.* Retrieved from https://www.teachthought.com/technology/7-ways-to-prevent-cyberbullying/

Giumetti, G. W., & Kowalski, R. M. (2019). Cyberbullying in schools, workplaces, and romantic relationships: The many lenses and perspectives of electronic mistreatment. Taylor & Franci

Gordon, S. (2022, July 22). *How to prevent cyberbullying*. Retrieved from How to Prevent Cyberbullying (verywellfamily.com)

Hirsh, C. L. (2023, January 10). *10 Effective tips on how to stop cyberbullying for kids and parents.* Retrieved from https://blog.mspy.com/how-to-stop-cyberbullying/

ICDL Arabia. (2016, April 5). *How-to-protect-yourself-from-cyberbullies.* Retrieved from http://onlinesense.org/how-to-protect-yourself-from-cyberbullies/

Kiplinger. (2023, May 11). *The Kiplinger Letter*, *100*(20), 4.

Lawrenz, L., Kolonko, C. (2022, July 8). *The mental health impacts of cyberbullying and how to cope.* Retrieved from https://psychcentral.com/blog/cyberbullying-the-psychological-effects-on-teens

Makad, S. (2018, March 6). *8 Important tips to fight against cyberbullying*. Retrieved from https:// https://thenextscoop.com/cyber-bullying/

MediaSmarts. (n.d.). *Strategies for fighting cyberbullying.* Retrieved from http://mediasmarts.ca/digital-media-literacy/digital-issues/cyberbulling/strategies-fighting-cyberbullying

Mehdi, K. P. (2020). *Encyclopedia of organizational knowledge, administration, and technology.* Hershey, Pennsylvania: IGI Global.

Norton. (2019, April 9). *10 Cybersecurity best practices that every employee should know*. Retrieved from https://us.norton.com/internetsecurity-how-to-cyber-security-best-practices-for-employees.html

Norton. (2020, September 30). *11 Ways to help protect yourself against cybercrime.* Retrieved from https://us.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html

Notar, C. E., Beard, L. A., Akpan, J. (2020). Cyberbullying: A new realm. *International Journal of Arts Humanities and Social Sciences*, *4*(4), 1-5. https://ijahss.in/Archive/vol-2issue-4/01-05.pdf

Notenboom, L. A. (n. d.). *What do I do if I'm being harassed, bullied, or stalked online?* Retrieved from https://askleo.com/what_do_i_do_if_im_being_harassed_bullied_or_stalked_online/

National Centre Against Bullying.(2023). *How to stop cyber bullying*. Retrieved (2023, May 3) from How to stop cyber bullying

Nelson, S. (2023, April 29). *How to stop cyber bullying.* Retrieved from https://www.wikihow.com/Stop-Cyber-Bullying

Net Nanny. (2016, March 28). *5 Ways to prevent cyber bullying*. Retrieved from https://www.netnanny.com/blog/5-ways-to-prevent-cyber-bullying/

NYC Public Schools. (2023). *Tools for keeping children safe online.* Retrieved from https://www.schools.nyc.gov/learning/digital-learning/applications-and-platforms/tools-for-keeping-children-safe-online

onelogin. (2023). *Six Types of password attacks & how to stop them*. Retrieved (2023, August 29) from (1) New Messages! (onelogin.com)

Pacer National Bullying Prevention Center. (2023). *Cyberbullying*. Retrieved from https://www.pacer.org/bullying/info/cyberbullying/

Parents editors. (2019, August 14). *How to stop cyberbullying: 18 Tips for parents and kids.* Retrieved from https://www.parents.com/kids/problems/bullying/18-tips-to-stop-cyberbullying/

Pavlovic, D. (2023). *10 Best ways to prevent cyberbullying online*. Retrieved (2023,May 3) from https://www.hp.com/ca-en/shop/offer.aspx?p=best-ways-to-prevent-cyber-bullying-online

Pew Research Center. (2022, December 15). *Teens and cyberbullying 2022*. Retrieved from https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/

Positive Action. (2023). *How to prevent and stop cyberbullying in schools: 6 Effective ways.* Retrieved (2023, May 8) https://www.positiveaction.net/cyberbullying-prevention

Safe Search Kids. (2023). *Protecting your child: Legal steps to combat cyberbullying.* Retrieved (2023, May 2) from https://www.safesearchkids.com/protecting-your-child-legal-steps-to-combat-cyberbullying/

Schifferle, L, W. (2015). *Technology tips for domestic violence and stalking victims.*

Retrieved from https://www.consumer.ftc.gov/blog/2015/02/technology-tips-domestic-violence and-stalking-victims

Security.org Team. (2023, January 26). *Cyberbullying: Twenty crucial statistics for 2023*. Retrieved from https://www.security.org/resources/cyberbullying-facts-statistics/#:~:text=According%20to%20our%20cyberbullying%20research,online%20during%20COVID%2D19%20lockdowns

Sequoia Alternative Program. (2023). *Preventing cyberbullying*. Retrieved (2023, June 12) from https://www.lrhsd.org/Page/3156

Spector, P. E. (2021). *Industrial and organizational psychology: Research and practice*. Hoboken, New Jersey: John Wiley & Sons.

Stopbullying.gov (2023). *What Is cyberbullying.* Retrieved (2023, June 26) from https://www.stopbullying.gov/cyberbullying/what-is-it

TeachThought Staff. (2015, March 9). *Ways to prevent cyberbullying.* Retrieved from https://www.teachthought.com/technology/7-ways-to-prevent-cyberbullying/

Tokunaga, R. S. (2010, May). Following you home from school: A critical review and synthesis of research on cyberbullying victimization. *Computers in Human Behavior, 26*(3), 277-287.

Twitter. (n.d.). *How to delete a tweet.* Retrieved from https://help.twitter.com/en/using-twitter/delete-tweets

United Nations Development Programme. (2023). *How to protect yourself from cybullying?* Retrieved (2023, May4) from http://indp.org/kazakhstan/how-protect-yourself-cybullying

Wall, T., Cooper, C. L., & Brough, P. (2021). *The SAGE handbook of organizational wellbeing*. **Thousand Oaks, California:** SAGE Publications Ltd

Webwise. (n.d.). *Schools, bullying and cyberbullying.* Retrieved from https://www.webwise.ie/teachers/schools-bullying-and-cyberbullying-2/

Whitson, S. (2014). *8 Keys to End Bullying: Strategies for Parents & Schools (8 Keys to Mental Health).* New York: W. W. Norton & Company

Zhu, C., Huang, S., Evans, R., & Zhang, W. (2021, 11 March). *Cyberbullying among adolescents and children: A comprehensive review of the global situation, risk factors, and preventive measures.* Retrieved from https://www.frontiersin.org/articles/10.3389/fpubh.2021.634909/full