SISHYA SCHOOL,HOSUR

ADVISORY TO PARENTS ON CYBER SECURITY/CYBER ABUSE ISSUES

There are some security threats aimed specifically at kids or teens, but most are aimed at any potential victim, regardless of age. Sometimes they just involve websites or subjects that interest a lot of kids, such as fan sites, YouTube, Instagram and other media-sharing services.

• **Kids love videos**. So malicious links can turn up in popular video-sharing sites like YouTube. Ask your children if they've ever seen links that could take viewers to inappropriate or illegal content in other sites and ask them what they do when they encounter them. Ads, too, can either link kids to content that isn't appropriate or scams and third-party sites that capture sensitive information. Young people need to be wary of "make a new friend" links, dating sites, and gossipy-sounding scams that look like invites from friends or tempt them to "find out who's talking about you" or "…who has a crush on you."

• **Kids often use family computers**. If children share a computer or device with parents, their online activities can affect all users, including any online shopping, banking or work parents do at home (be careful when logging into your work network from a shared computer). And parents will want to be aware that, if kids check browser history, they can be exposed to sites their parents visit on the family computer.

• **Kids can be big fans**. There are lots of celebrity sites, and the ones operated by the celebrities themselves or entertainment news publishers are fine. But kids need to be extra wary of fan sites that turn up in search results but aren't actually run by the celebrities and the people who cover them. It's not always easy to tell, but at least they're usually lower down in the search results.

• **Kids are social**. There are social reasons why kids are hacked. One form of bullying is using a password a child has shared to break into his or her social media account and post embarrassing messages or images or use the account to spread spam or post links to malicious sites. Teach your kids not to share passwords, even with their closest buddies, and always to close out of accounts when they're finished using computers shared with other people

• **Kids' IDs** are valuable to thieves. It may surprise you that kids are sometimes the target of identity theft – where a criminal gets enough information about them (e.g., name, address and social security number) to apply for credit or commit a crime in a child's name.

www.connectsafely.org/wp-content/uploads/**security**guide.pdf

Dealing with Cyberbullying
Tips for Kids and Parents to Prevent and Stop Cyberbullying

Technology means that bullying is no longer limited to schoolyards or street corners. Cyberbullying can occur anywhere, even at home, via email, texts, cell phones, and social media websites 24 hours a day, seven days a week, with potentially hundreds of people involved. For those who suffer cyberbullying, the effects can be devastating, leaving you feeling hurt, humiliated, angry, depressed, or even suicidal. But no type of bullying should ever be tolerated. These tips can help you protect yourself or your child online and deal with the growing problem of cyberbullying.

What is cyberbullying?

Cyberbullying occurs when a child or teen uses the Internet, emails, text messages, instant messaging, social media websites, online forums, chat rooms, or other digital technology to harass, threaten, or humiliate another child or teen. Cyberbullies come in all shapes and sizes—almost anyone with an Internet connection or mobile phone can cyberbully someone else, often without having to reveal their true identity. cyberbullies can torment their victims 24 hours a day and the bullying can follow the victim anywhere so that no place, not even home, ever feels safe, and with a few clicks the humiliation can be witnessed by hundreds or even thousands of people online.

How cyberbullying harms

The methods kids and teens use to cyberbully can be as varied and imaginative as the technology they have access to. It ranges from sending threatening or taunting messages via email, text, or IM to breaking into your email account or stealing your online identity to hurt and humiliate you. Some cyberbullies may even create a website or social media page to target you.

As with traditional bullying, both boys and girls cyberbully, but tend to do so in different ways. Boys tend to bully by "sexting" (sending messages of a sexual nature) or with messages that threaten physical harm. Girls, on the other hand, more commonly cyberbully by spreading lies and rumors, exposing your secrets, or by excluding you from emails, buddy lists, or other electronic communication. Because cyberbullying is so easy to perpetrate, a child or teen can easily change roles, going from cyberbullying victim at one point to cyberbully the next, and then back again.

The effects of cyberbullying

Any type of bullying can make you feel hurt, angry, helpless, isolated, even suicidal, or lead to problems such as depression, anxiety, and low self-esteem. In many cases, cyberbullying can be even more painful than face-to-face bullying because:

- Cyberbullying can happen anywhere at any time, even in places where you normally feel safe, such as your home, and at times you'd least expect, such as at the weekend in the company of your family. It can seem like there's no escape from the taunting and humiliation.
- A lot of cyberbullying can be done anonymously, so you may not be sure who is targeting you. This can make you feel even more threatened and can embolden bullies, as they believe online anonymity means they're less likely to get caught.
- Cyberbullying can be witnessed by potentially thousands of people. Emails can be forwarded to hundreds of people while social media posts or website comments can often be seen by anyone. The more far-reaching the bullying, the more humiliating it can become.

Respond to cyberbullying by:

- **Saving the evidence of the cyberbullying,** keep abusive text messages or a screenshot of a webpage, for example, and then report them to a trusted adult, such as a family member, teacher, or school counselor. If you don't report incidents, the cyberbully will often become more aggressive.
- **Reporting threats of harm** and inappropriate sexual messages to the police. In many cases, the cyberbully's actions can be prosecuted by law.
- **Being relentless.** Cyberbullying is rarely limited to one or two incidents. It's far more likely to be a sustained attack on you over a period of time. So, like the cyberbully, you may have to be relentless and keep reporting each and every bullying incident until it stops. There is no reason for you to ever put up with cyberbullying.
- **Preventing communication from the cyberbully,** by blocking their email address, cell phone number, and deleting them from social media contacts. Report their activities to their internet service provider (ISP) or to any social media or other web sites they use to target you. The cyberbully's actions may constitute a violation of the website's terms of service or may even warrant criminal charges.

Spot the warning signs of cyberbullying

Your child may be the victim of cyberbullying if he or she:
- Becomes sad, angry, or distressed during or after using the Internet or cell phone.
- Appears anxious when receiving a text, IM, or email.
- Avoids discussions or is secretive about computer or cell phone activities.
- Withdraws from family, friends, and activities they previously enjoyed.
- Suffers an unexplained drop in grades.
- Refuses to go to school or to specific classes, or avoids group activities.
- Shows changes in mood, behavior, sleep, appetite, or shows signs of **depression** or anxiety.

Monitor your child's technology use

Regardless of how much your child resents it, you can only protect him or her by monitoring what they do online.

- Keep the computer in a busy area of your house so you can easily monitor its use, rather than allowing your child use a laptop or tablet in his or her bedroom, for example.
- Give your child a simple phone as a device to receive calls or call up important people.
- Set up filters on your home computer. Tracking software can block inappropriate web content and help you check up on your child's online activities.
- Insist on knowing your child's passwords and learn the common acronyms kids use online and in text messages.
- Know who your child communicates with online. Go over your child's address book and instant messenger "buddy list" with them. Ask who each person is and how your child knows them.
- Encourage your child to tell you or another trusted adult if they receive threatening messages or are otherwise targeted by cyberbullies, while reassuring them that doing so will not result in their loss of computer or cell phone privileges.

http://www.helpguide.org/articles/abuse/cyberbullying.htm