CYBER LAW TERMINOLOGIES – PARENTS BE AWARE

By Dr. Sapna Sukrut Deo[247]

Internet is proving to be a boon to us as it is helpful for us in many ways. But it has its own risks too specially when children are its users. Today large number of population is active on social networking sites like Facebook, Twitter, Orkut, Myspace etc. where we do share our information and pictures. In fact even kids nowadays have their own profiles on these sites. The problem here is in this kids do share their personnel information as in which school they go, their address etc. which can be used by internet predators or criminals. Then there are porn sites which we don't want our kids to visit. In fact even most of the time on normal sites too we do spot porn sites advertisement appearing. This may generate curiosity in a kid to watch it. We cannot deny our child internet access. They have to because it is required to do school projects. Secondly in today's age it is necessary to have computer and internet knowledge. In this article I want to discuss how the internet can do harm to the children and also the safety measures which the parents should share with their children.

The Dangers of The Internet :

- The good thing about the internet is that there are so many websites to choose from. That is the reason why it is a good way to research school projects. With that said, having so many websites to choose from can be dangerous. The child can gain access to social networking websites, adult chat rooms, pornographic websites, and websites that are violent in nature.
- It is easy and convenient to make friends online but it is much different than doing so in person. Because we don't know who really is on the other side. The internet makes it easy for someone to be anyone else in the world.
- As stated above, the internet makes it easy to create a new, false identity. Often times, the individuals who lie about their ages are internet predators. They often target children. And try to approach the child or contact them in person. What many parents do not realize is that children and teenagers can easily become targets of online child predators. Many also do not realize that this process doesn't always happen

[247] Assistant Professor, Bharati Vidyapeeth ,New Law College, Pune.

overnight. Some child predators pretend to be the ages of their targets. They then work to gain the trust of those targets. This can take a few days or a few weeks.

- Many individuals, including both children and parents, do not know that the information that is posted online isn't always private. For starters, most teens have their profiles set to public, as opposed to private. This means that anyone can view it. There are also online message boards that are indexed by the search engines. This means that others can view the conversations that were discussed.
- Childs are the one who have control of internet when they use it. If the child is older and mature, it is okay but honestly we never know. We may ask our child not to communicate with strangers online, give out their phone numbers, or share pictures with strangers, but that doesn't mean that they will follow the rules. For that reason it is better to monitor their use.
- A child may get involve in doing something they shouldn't be doing online, like having direct, personal conversations with a stranger, who may be a child predator. If they automatically shut off the computer or put a game on the screen, they may be trying to prevent you from seeing what they are doing online.
- The teenagers while communicating with someone online may get in the process of starting a relationship, which they are happy about. Unfortunately, many teenagers do not realize that anyone can hide behind a computer. This is dangerous of starting an online romance.
- Many teenagers use the internet for harassment. If your teenager has a falling out with one of their friends, they may find themselves being harassed online.
- While doing online shopping kids can share personal information such as bank account and credit or debit card information. This can be used by a hacker too. Or in fact can be misused by the child too. Like of doing unnecessary shopping or spending huge amount etc. Better to tell them not to do it without your approval.
- Phishing, hacking, cyber-bullying, Facebook depression, sexting, paedophiles, scammers and exposure to inappropriate content gives the child an idea of what internet dangers are all about.

Safety Measures :

- Teach your child to never give out personal information online like your phone number; address; name or location of your school or your password. And if they think it is necessary to give some information to check with you first.
- When children participate in an online activity where a log on name or user name is required, parents should help them come up with a suitable name and make sure it doesn't reveal any personal information.
- Tell them to always keep their online account id and password private, except from you. And not to share it with friends even the best friend. To change the password if you think someone else knows it.
- Nothing online is completely private. Tell them to think about what they write in chat rooms, emails and instant messages. If personal information, provocative photos or intimate details are sent to friends, to remember that even friends can use this against or cause problems later on.
- Not to meet an 'online' friend in person. This person might cause harm. There are bad adults that pose as kids. If there is someone to must meet make sure they go with you and make the meeting in a public place.
- Ask them to check with you before downloading or installing software. Do not open attachments from emails you don't recognize even if they are addressed to personally. It could let in a virus, damage the computer or put your family's privacy at risk.
- Not to share photos of with anyone you don't know. Don't share provocative photos of yourself or friends once they are out there you cannot control who sees them.
- Visit areas on the web that is appropriate when surfing online. Visiting inappropriate areas can put at risk and lead to trouble. Use your computer responsibly and know that your usage can be tracked.
- Always remember to log off at any time! Decide how long should be spend on computer each day and log off when the time is up. There is a whole world out there one can't be fit and healthy if he sits in front of computer all day.
- To respect other people's property online. Illegal copying of music, games, movies, software and so forth is theft in the same way as stealing something in a store.
- Parents should keep themselves oriented on their children's use of Internet. Children should share their experiences online with their parents.
- Block the websites that you want to keep your child away from. For example, if you asked your child or teenager not to post personal pictures or videos of themselves

online, but they still continue to do so, block the social networking websites that they use. If you have Internet Explorer, this is easy to do. First, open a new internet window. Then, from the dropdown menu select "Tools", and then "Internet Options", and then click on the "Content Tab". Finally, under the heading of "Approved Sites", you can also enter in the websites you want blocked.

- Many wireless carriers offer content filtering features that help block access to mobile sites with mature content as well as filter out inappropriate sites from search results.
- Due to the Web's potential dangers, many service providers offer free tools and software to help restrict certain types of content and features to keep young Web users safe.
- **Internet service providers (ISPs)** like Verizon, AT&T and Comcast offer such free parental control features as the ability to:

1. Get a Web activity report that shows you all the Web sites your children visit or attempt to visit. You can check out the sites your kids have visited and block specific sites or types of sites you don't want them going back to.

2. Create unique profiles for different family members with individualized online usage limits. This can be useful if you have children of different ages. One master account can be used to manage the settings of several subordinate account users.

3. Block access to certain Web tools such as instant messaging, gaming, chat rooms, and message boards, allowing parents to keep better track of what their children are saying and to whom.

4. Remotely manage your account with the ability to change parental control settings from any computer with Web access, whether in or outside the home.

5. View your child's online activities as they happen with real-time Web tracking features

6. Allow young Web users to request permission to visit unauthorized Web sites for an adult to approve.

7. Receive a tamper controls alert if someone other than you tries to change the control settings.

8. Set up a timer that limits the amount of time users can spend online.

9. View search monitoring results that track the words and phrases your children search for online to help learn about what they are interested in. This way you can find out if they are trying to seek out blocked or inappropriate content.

10. You can also set up similar controls on the Internet browsers and search engines (Internet Explorer, Firefox, Safari, Google Chrome, etc.) level. Most browsers let you restrict access to certain sites or pre-approve a list of sites your child has the ability to access. For example:

1. Safari users can create child user accounts that let you choose between three levels of Internet access:

   a. give your children unrestricted access to all sites

   b. a setting that only blocks access to certain restricted sites

   c. an option that only lets children access sites you that you have pre-selected. Email and chat features can be set up so that young users can only chat and email with contacts you know and trust. Weekday and weekend computer time limits can be put in place as well.

2. Firefox and Chrome have no built-in parental control features. But, if your computer uses one of these browsers, you can download extensions such as ProCon (which blocks accidental visits to adult sites), LeechBlock (which sets up time limits for different users), and FoxFilter (which blocks content based on user-defined criteria).

3. Search engines like Google and Bing have "safe search" settings that screens for sites that contain explicit sexual content and deletes them from your search results. This can be a great option since kids often stumble upon inappropriate content by accident when searching seemingly innocent terms.

Above are just few exhaustive measures you can take to ensure internet safety of your child. But most importantly it is important for us to have thorough knowledge of computer and

internet usage. There are plenty of classes or courses you can opt for to gain computer and internet knowledge. Do ensure that your computer is faced towards a space where you can easily see what your child is doing. Be aware yourself and let your child use the internet. Because it is a need of a time to use internet so, don't let your child lack behind because of these fears. An open conversation on pros and cons will solve your problem.