Health Class – Internet Safety (from www. Safekids. com)

What are the risks?

•Harassment and bullying

Just as has been going for eternity, some kids are mean to other kids. On social networking sites and apps or via email or text messages, children sometimes encounter messages that are belligerent, demeaning, harassing, annoying or just plain mean.

For the most part, cyberbullying is the same as regular bullying and often both occur at the same time (kids who are bullied online or via phone are often also bullied at school, usually by the same people). And, while bullying can be extremely harmful, not all negative interactions online rise to the level of bullying, which typically is defined as repetitive and where there is a power imbalance. Sometimes what adults consider bullying is what kids see as "drama." Not every snide comment, innuendo or joke at another's expense requires an adult intervention.

•Posting material that could harm your reputation

How you present yourself online is a reflection of you. ***Whether it's being mean to others or being seen in photographs where you are dressed inappropriately or doing something that could embarrass you now or in the future, there are situations that can haunt you for a very long time***. Anything digital can be copied, stored and pasted so even though you think it's been deleted, there is a chance that what you post online could follow you for a long time. Still, it's a good idea to look around for anything about you or your kids online that you might want to take down before it's seen by the wrong people. Facebook and other social networks have tools that allow you to review and remove posts and pictures that could embarrass you in the future. Consider using a search engine to see what's been posted publicly by and about your kids. Most teens have heard about the risks associated with inappropriate posts (especially those applying for college) but it never hurts to have a discussion about this and to be a good role model by making sure your own posts (and those with pictures of your kids) are suitable for just about anyone who might see them.

• Security risks

There are a variety of security risks ranging from downloading files that contain malicious software that can jeopardize your privacy or financial data, to social engineering scams that trick people into giving up personal information including passwords and credit card numbers. The best way to protect yourself and your children is for you and them to think critically about the information you provide. ***If you get an email that asks you for a password and user name, question whether it's legitimate and — even if you think it is — don't click on any links, but type in the address of the site yourself to avoid getting caught up in a "phishing" scheme. Make sure you and your kids have secure passwords and that they know to never give them out to anyone, even their best friends.*** The one exception is for young kids to share their

passwords with their parents. Be sure that your devices' operating systems are up-to-date and use up-to-date security software. Be very careful about any apps you install on a smartphone or software you download on a computer.

Also be on guard for identity theft where someone steals just enough information to be able to impersonate you or your child. It turns out that children are often victims of identity theft because they almost always have perfect credit records so — by impersonating them — it's possible to borrow money in their name. Also beware of impersonation on social networks where others post embarrassing, distasteful, mean and potentially even illegal content in your child's name.

•Privacy

There are lots of ways that a child's privacy could be at risk. The biggest is *what they post themselves*. If something is really embarrassing or simply shouldn't be shared with the public, then don't put it online.

Talk with your kids about the privacy tools on social networks. Most allow you to restrict who can see your posts but be aware that even posts that are private can be copied and shared by others (rude though that is). For more on social network and app privacy, see ConnectSafely's parents' guides.

Another privacy risk is *third party tracking cookies* and other techniques that hone in on your interests and target you with advertising and offers. There are ways to minimize the ability of companies to track you online (some browsers have settings to help prevent it) but it's hard to avoid completely. Also, as annoying as the ads may be, it's the price we pay for all the great free services and content out there. It's very unlikely that a tracking cookie can affect your or your child's safety, especially if they come from reputable sites.

Mobile apps: Pay close attention to the mobile apps your kids are using. What information do they collect? Some apps track your child's location, others seek permission to post publicly on their user's behalf. Many routinely ask "permission" for all sorts of information when you install them so it's a good idea to review the apps and what information they are collecting or passing on.

•Legal and financial risks

A child could do something that has negative legal or financial consequences such as giving out a parent's credit-card number or doing something that could get them in trouble with the law or school officials. That can even include "sexting," taking and sharing nude, partially nude or sexually provocative pictures of themselves that can violate child pornography laws and other statutes. Legal issues aside, children should be taught good "netiquette" which means to avoid being inconsiderate, mean, or rude.

•Exposure to inappropriate material

A child may be exposed to inappropriate material that is sexual, hateful, or violent in nature, or encourages activities that are dangerous or illegal. Children could seek out such material but may also stumble on it if they're not looking for it. If you think your child may be looking at pornography, take a deep breath and think about how you should react. For more, see So your kid is looking at porn. Now what?

•Online predators and physical molestation

Although it can happen, the risk of a child or teen being harmed by someone they met on the Internet is very low. There has been widespread misunderstanding of a 2005 study that found that 1 in 7 youths had received an unwanted online sexual solicitation but the authors of that study — the Crimes Against Children Research Center — posted a fact sheet that explains that these solicitations are typically not from predators and most of the recipients of the solicitations did not view them as serious. "Most were limited to brief online comments or questions in chat rooms or instant messages. Many were simply rude, vulgar comments," and "Almost all youth handled unwanted solicitations easily and effectively." It's certainly a good idea for children and teens to be careful when communicating with people they don't know in person and, if the conversation starts to be about sex or physical details, that's a very good time to bail out. Research has shown that talking about sex with strangers is one of the most dangerous things a young person can do online.

While it's generally OK to post appropriate pictures, school name or the city you live in, kids should avoid posting their home address and, if they do post their phone numbers and email addresses, it should be restricted only to actual friends.

Children should be cautioned not to get together with someone they met online. If, for some reason, a meeting is arranged, make the first one in a public place. And be sure to accompany your child. If you do suspect that your child is being contacted by an adult for sexual reasons, contact your local police and then report it to the CyberTipline online or by calling 800 843-5678.
For more on the facts and myths beyond Internet predators, see Predator Panic Making a Comeback.

How parents can help reduce risks

Filters and monitoring tools

While technological-child-protection tools are worth exploring, they're not a panacea. To begin with, no program is perfect. There is always the possibility that something inappropriate could slip through or something that is appropriate will be blocked. Also, filtering programs do not necessarily protect children from all dangerous activities. And even though they might block what children can *see* online, they might not block what they can *say*. For example, even with a filter it might be possible for a child to post inappropriate material or personal information on a social networking site or blog or disclose it in a chat room or instant message. Also some filters do not work with peer-to-peer networks that allow people to exchange files such as music, pictures, text, and videos. Filters are not a substitute for parental involvement. Regardless of whether you choose to use a filtering program or an Internet rating system, the best way to assure that your children are having positive online experiences is to stay in touch with what they are doing. The best filter — the one that lasts a lifetime — doesn't run on a device but on the software between your child's ears.

Useful Apps :

Web of Trust and Avast ! Antivirus