

Summary of Social Media/Protections Program given by Jeff Sunseri, Karen watt of Mt. Aloysius College and Bill Latchford of Penn State University, founder of [www.protectchildrenonline.org](http://www.protectchildrenonline.org)

Online risks:

- Strangers/criminals who pose as teen friends, gain trust, ask for pictures, info or meetings - with intent to harm.
- Friends or acquaintances who bully online anonymously so you can't fight back.
- Teens themselves - can post pictures or statements that come back to hurt them 10 years later when applying for jobs.

Protection steps:

- Educate your kids about the dangers
- Have a dedicated computer for kids to use and keep it in a high traffic area of the home. Each child needs a non-privileged account so parents can track their activity.
- Mobile devices - create a central family charging station where kids put devices when not in use and set hours when devices can be used.
- Have Computer Rules - Set agreed upon rules and post next to computer.
- Use parental controls & software safeguards for younger kids.
- Kids should never get in trouble with parents for telling them about a website that popped up or was accidentally visited. Open communication builds trust.

Visit websites:

<http://securingthehuman.sans.org/resources>

<http://www.protectchildrenonline.org/>

<https://www.onquardonline.gov/topics/protect-kids-online>

<https://account.microsoft.com/family/about>

<http://windows.microsoft.com/en-us/windows/set-parental-controls#1TC=windows-7>

<https://www.facebook.com/safety/groups/parents/>

<https://www.opendns.com/home-internet-security/>

<http://techessentials.rogers.com/tipsforparents/FiveParentalControl.aspx>