



## Top 10 Lessons Parents Can Help Reinforce At Home:

1. Passwords should be at least 8 characters in length, and should include numbers, symbols, and a combination of upper and lowercase letters. Passwords are private and should only be shared with a parent.
2. A child's online username should never reveal his/her name, age, gender, phone number, address, password, or school.
3. Children should never open an email from a stranger or reply to an email or a text from a stranger.
4. Personal pictures should not be posted online or used for an online profile picture. Personal pictures should not be shared in a text or in an email with strangers either.
5. Children should never agree to meet someone they have only met online.
6. Children should never respond to emails, texts, or postings that are mean, inappropriate, or that make them feel uncomfortable. They should ask a trusted adult for help instead.
7. Online written communications should be polite, respectful, and free of sarcasm since a person's body language and intent can't be judged in an online environment.
8. Be a good friend and never post anything online about your friends that could make them feel bad. Also never post pictures of your friends online without receiving their permission first.
9. Don't engage in cyberbullying. If you are the victim of cyberbullying, or know a friend who is being cyberbullied, immediately ask a trusted adult for assistance and advice.
10. Closely evaluate websites when you feel the information that you have found could be inaccurate. Don't believe everything that you read online.

## Additional Thoughts To Keep In Mind At Home:

**Start young.** Using age appropriate vocabulary, talk with your child about online behavior, safety, and security as soon as he/she begins using the Internet.

**Parents are a child's primary role model.** Consider how you use personal technology and what you do and say online since your child is always watching and learning from you.

**Keep your ears open.** Encourage your children to share everything they do, see, and hear online with you. Create a plan for what your child will do when he/she comes across something online that makes him/her uncomfortable or scared.

**A digital footprint can remain online for a very long time, even after a posting has been deleted.** Once something has been posted online, it can be copied and sent to hundreds of other people without your knowledge. Remind your child to always "think before you click".

**Delete unwelcome attachments and keep your virus and security software up-to-date.** Teach your child that attachments from unknown sources should be treated with suspicion. While they can be effective when kept up-to-date, virus and security software should not be relied upon solely to protect your machine.

**Enable parental controls.** Most computer operating systems allow the parent's administrative user account to set online restrictions on other standard user accounts.

**Set time limits.** The American Academy of Pediatrics recommends limiting total screen time in front of a computer, handheld device, or a TV to no more than 1-2 hours a day. Such time limits can be set using parental controls on many computers and other devices.

**Utilize the Bookmarks Bar and Menu.** Become familiar with the web sites your child is visiting often and bookmark them for easy access, thus avoiding typos and spelling mistakes that could yield inappropriate sites.

**Computers should be located in a central area of the house.** Whenever possible, computers should be located in high-traffic common rooms of your house, with the screen facing the interior of the room.

**Mobile device management can be a moving target.** Smartphones and many handheld devices have built-in web browsers. Since they are small and mobile, it is harder to monitor what your child is doing on them. Make very clear what your expectations are on such devices and remind your child that you have the right and the responsibility to review their online activities if a concern ever exists.

**Establish "no device" zones and times.** Laptops and smartphones should generally not be used during mealtimes and other times when a family is sitting together. Consider using a common area on the first floor to collect smartphones during homework, and especially when charging them at bedtime.

**Remind your child "it can wait".** Children suffering from Fear Of Missing Out (FOMO) often need support and reassurance that they don't need to check their social media 24/7.

**Gaming is more addictive and immersive than ever before.** Research the games your child wants to purchase, paying close attention to online opportunities, especially when your child could be playing the game with a headset.

**Be vigilant outside the house as well.** Determine what kinds of computer safeguards are utilized at the homes of your child's close friends, as well as other locations where your child might use technology unsupervised.

**Contact your ISP.** Most Internet Service Providers offer free or low-cost products that can contribute to online security at home.

