**Internet Safety Tips for Parents and Students**

**Internet Safety Tips:**

Social networking sites, chat rooms, virtual worlds, and blogs are how teens socialize.  Below are some tips to help your child navigate these spaces safely.

* Keep computers in a high-traffic area of your home.
* Establish limits for which online sites children may visit and for how long.
* Use privacy settings to restrict who can access and post on your child’s profile.
* Review your child’s friends list.
* Remember that Internet technology can be mobile, so make sure to monitor cell phones, gaming devices, and laptops.
* Explain to your kids why it’s a good idea to post only information that they feel comfortable with others seeing.
* Remind your kids that once they post information online, they can’t take it back.
* Encourage your kids to trust their gut if they have suspicions. Know who is connecting with your children online and set rules for social networking, instant messaging, e-mailing, online gaming, and using webcams.
* Continually dialogue with your children about online safety.

Many federal agencies offer free tutorials, resources and guidelines for parents.  The National White Collar Crime Center offers free video tutorials for parents.  Some of their helpful tips include:Be a good role model on and offline.

* Focus on your family, not your phone.
* Know what your teens are doing online.
* Be mature on social media.
* Set aside “tech free time” every day.
* Be someone teens can talk to.
* Make talking and listening part of everyday.
* Listen to the good and the bad.
* Know that their feelings are real.
* Be strong in crisis.
* Stay calm.
* Know when to call 911 and when to call the school.
* Don’t wait for someone else to act.
* Keep records.

Also be aware of Phishing and ways to prevent it.  According to the [OnGaurdOnline.gov](https://www.consumer.ftc.gov/features/feature-0038-onguardonline), Phishing is when scam artists send text, email, or pop-up messages to get people to share their personal information. Ways you can avoid phishing:

* Don’t reply to text, email, or pop-up messages that ask for personal information.
* Don’t give personal information on the phone in response to a text message.
* Be cautious about opening any attachment or downloading any files from emails you receive.
* Use security software and update it regularly.