

## Internet Safety Tips for Families

Technology helps us stay connected to loved ones; helps us learn; helps us do our jobs; entertains us; and makes life easier through online banking, shopping and other activities. It also has the potential to make us vulnerable. Cyber criminals, identity thieves, and others often use the Internet to identify and target their victims. So, as technology plays an ever larger role in our lives, at an ever younger age, you may be wondering how to keep your family safe online. The following are internet safety tips that were shared by several attendees at February's PTA meeting. This is by no means an all inclusive list, but these are items that frequently appear in media reports on Internet safety.

- Keep your computer(s) in a "public" space within your home where you can monitor your child(ren)'s online activities.
- Consider password protecting your computers and/or internet accounts so that you will have to assist your child(ren) in getting online and can better monitor their online activity.
- Likewise, consider password protecting your online shopping accounts and not saving those passwords on your computer.
- Make use of child-friendly search engines. Even seemingly innocuous search terms will often produce search results that are graphic in nature and inappropriate for children. Child-friendly search engines exist and have been designed to try to screen out these inappropriate results. Ms. Safford, Stonegate's Media Specialist, provided attendees with the following list of child-friendly search engines and research sites that you may wish to consider using:
  - Yahoo for Kids: [kid.yahoo.com](http://kid.yahoo.com)
  - Quintura for Kids – [kids.quintura.com](http://kids.quintura.com) (Be sure to start with the "quick tour" near the bottom of the page.)
  - Kids Click – [www.kidsclick.com](http://www.kidsclick.com)
  - Ask for Kids – [www.askforkids.com](http://www.askforkids.com)
  - Clusty – [www.clusty.com](http://www.clusty.com) (results sorted by category – not especially for kids)
  - SweetSearch – [www.sweetsearch.com](http://www.sweetsearch.com) (sites reviewed by educators)
  - Videos for "all ages" – [www.wimp.com](http://www.wimp.com)
  - Searchable Videos for Kids – [video.kidzui.com](http://video.kidzui.com)
- What is posted on the Internet stays on the Internet. Once something is posted on the Internet, it is there forever. While you may "take it down", hide it from view, or otherwise remove it from the site where you posted it, it is impossible to delete something completely from the

Internet. Once posted, it will be stored on servers; cached in memory; copied or linked to another web site, etc. Just because you removed it from view in some manner, does not mean it's no longer there.

- Read the user agreements for sites before you “agree” to them. We all do it – the font is tiny and the document is long, so we skip over the user agreement for that new photo sharing or social networking site we want to sign up for. We simply click “accept” and move on. However, many of those user agreements tell you that once you post a photo to the site, the site has the right to use any photos you post however they want. That means your photo could end up on the next commercial for that website or on the landing page where users sign-in to the page.
- Consider not posting individual photos of your child(ren) online. For those who prey on children online, it is easier to alter photos of an individual than to isolate and alter a single person in a group photo. Save the individual photos for direct e-mails to family members or hard copy distribution.
- Know your devices. Portable electronic devices and the many applications they use have features and capabilities that, while tremendously helpful, also potentially put the user at risk. These capabilities can often be disabled, but to do so, you need to know which capabilities your device has so that you can decide which, if any, pose risks. Two examples:
  - GPS is a great tool that is now in just about every portable electronic device you buy (phones, cameras, iPods and other music players, digital cameras, etc.). However, those GPS-enabled devices track your movements and geo-tag photos taken with the device. Geo-tagging refers to embedding the geographic location (latitude and longitude) where the photo was taken in the metadata of a photograph. What this means is that posting to a social networking site or photo sharing site from a GPS-enabled devices potentially exposes your location (or the location where the photo was taken). For those who know how to access the metadata this locational information can be a gold mine.
  - In-app(lication) purchases – Many applications (aka apps) downloaded onto portable electronic devices, such as games, are free or very low cost, but offer opportunities to purchase items within the app to enhance the user’s experience. For example, the ability to purchase items to decorate your virtual house in a game on your smartphone. These in-app purchases can become very costly, very quickly, and children do not always understand that they are actually spending real money. Consider password protecting or blocking the ability to make in-app purchases on your device.
- If you or your children engage in social networking on sites such as Facebook, MySpace, Twitter, and FourSquare, there are a number of things you can do to make the experience more secure.
  - Use your privacy settings. “Friends-only” is a good setting because most people are relatively familiar with the individuals on their “friends” list. However, each

progressively more open setting (e.g. friends-of-friends) opens your profile to more individuals that you may not actually know in-person.

- Check your privacy settings regularly as many sites default all user's privacy settings back to "open" frequently.
  - Only "friend" or accept "friend" requests from individuals you have met in-person. It is very difficult to determine someone's true identity if you have only met them online.
  - Think twice about posting location information. Posting frequent updates on your location allows someone who may be following you or your child establish your routines and habits making you more vulnerable to stalking and other criminal activity. Providing detailed times of your daily comings and goings also gives criminals a sense of when your home may be vacant and vulnerable to burglary.
  - Finally, talk to your children about Internet safety. Much of the same guidance you give to your children about talking to people in-person applies online. What do you want them to say (or not say). Topics to consider are: full name, address, phone number, parents' names, where they go to school, where you work, family schedules, etc. If you don't want them to share certain information, tell them. Set clear ground rules for computer use and the Internet safety rules you expect them to follow.
- Conduct an Internet search on yourself and your children periodically. It is always good to know what is publically available about yourself.
  - Use Internet security software that protects from a variety of virus, spyware, and malware threats and use it consistently. Set it to run all the time in the background, to update the threats it looks for automatically, and to run a full system scan on a regular (e.g. weekly) basis.