Officer Scott Driscoll heightens awareness of internet safety for children

By Marianne Wallace on May 25, 2013 in Schools · 0 Comments

About author

Marianne Wallace

Recently, the Wilton PTA Council, Wilton High School PTSA, and Wilton Youth Council co-hosted a talk by Scott Driscoll, a law enforcement officer with 24 years of experience. He shared eye-opening stories from the national news and his own career to heighten parents' awareness of the issues and dangers their children can be exposed to when using the Internet. He offered the following tips for Internet safety.

No. 1: Restrict the use of your network to family members and don't share passwords to accounts or networks with your friends. Have your password protected and change it periodically.

All emails and files sent from and received by your computer or network have an IP address associated with them which is basically like a "phone number" for your computer or network. If someone uses their laptop or other electronic device to access your wi-fi network and downloads illicit files, these can be traced back to you and your network.

No. 2: Avoid Peer-to-Peer file-sharing sites which connect users to either central computers or directly to other users' computers to download and share digital files over the Internet.

Use of these sites puts you at risk of computer viruses. He suggested staying away from "free" file sites such as BitTorrent, BitComet, Shareaza, uTorrent, Bear Share, Ares Galaxy, BitLord, and FrostWire. It's safe to stream and download from sites like Pandora, iTunes, and Spotify.

No. 3: Stay away from video chatting sites such as Omegle, ooVoo, and Chatroulette. Video chatting is like inviting a stranger into your home. Child predators visit these sites, he said. It's best to keep computers and devices in common areas and out of bedrooms. Parents also need to limit and supervise Internet use as well as impose age-appropriate controls (e.g., Net Nanny, Spectra Pro, Cyber Security Pro).

No. 4: Remind children to never share any personal information online, especially when playing Internet-based games or gaming systems such as Minecraft, Wii Nintendo, Xbox 360, PS 3, and PlayStation. There is no filter on these public networks.

Your "digital footprint" provides data on everything you have done in the digital environment (e.g., what you clicked on, searched for, Liked, where you went, your current location, your IP address, what you said, what was said about you, etc.).

No. 5: Use smart phone settings to turn off the GPS and GED tagging functions tied to the camera. They can give predators Meta data information on a child's location.

No. 6: Be careful about posting and tagging photos on Facebook. Colleges and employers can Google a child's name and email address and learn or make assumptions about them from photos.

No. 7: Facebook accounts can never be deleted. They can only be deactivated. Twitter conversations can be deleted.

No. 8: Never make "anonymous" postings on anyone's Facebook page or website. Be sure children learn not to say or do anything online that they would not say or do in person.

No. 9: Avoid "sexting" — sending sexually explicit messages or photos via Snap Chat, Facebook Poke, and Instagram. Although how long a photo may be viewed may be limited, that does not prevent someone from grabbing a screen shot and sharing it.

No. 10: Beware of cyber bullying — use of the Internet to harm other people in a deliberate, repeated, and hostile manner. The results can be catastrophic. If a child experiences cyber bullying of any kind, encourage them to tell a trusted adult immediately.

Mr. Driscoll has written a book, *www.R U in Danger.net*. It and more information are available through his website, InternetSafetyConcepts.com.