keeping our kids cyber-safe

AN ORADELL PUBLIC SCHOOL PARENT ACADEMY WORKSHOP

Online Safety Advice from Computer Crimes Expert Brian Sinclair

As head of the Bergen County Prosecutor's Office Computer Crimes Task Force, it is Brian Sinclair's job to investigate how Internet and mobile technologies can be misused to the detriment of Bergen County children.

But Sinclair's work doesn't end there. He is simultaneously dedicated to educating the community about cyber-safety strategies in hopes of preventing senseless cases from crossing his desk down the road.

"I have always felt that students, parents, and teachers need to be educated about what these devices can do," said Sinclair. "Technology isn't good or bad. It is just another thing that can be manipulated and used improperly. The mission of my office is to get this message out to the public."

On April 24th, Sinclair visited Oradell Public School to do just that, speaking with parents about keeping children "cyber-safe" as part of the school's Parent Academy Workshop series. Earlier that week, Sinclair also led an assembly attended by fifth and sixth grade OPS students and teachers. The focus of that program was what students can do to protect themselves online. Topics included online predators, social media mistakes, and cyber-bullying, among others.

"Our administrative team was amazed when 90-percent of our fifth and sixth grade students shared that they utilized some form of social media," said Oradell Public School Principal Megan Bozios. "Technology is finding its way into children's hands at younger ages. We need to work together as a community to ensure that they have the tools and knowledge to stay safe."

All parents worry about "stranger danger" and take steps to safeguard their children's physical well-being. During his presentation, Sinclair cautioned that the same level of vigilance should be applied to children's activities online. Where is your child going on the Internet? With whom is he or she interacting? And, importantly, what information is being shared – intentionally, as part of an online profile and, inadvertently, through photos being posted on Web sites and apps?

(continued on page 2)

Making Your Home a Safe Haven

"There are three doors to your house: the front door, the back door, and the door to the Internet," Sinclair said. "If you remember to lock the first two but leave that last door open, your home is not a safe haven for your child."

Showing a photographic collage of convicted online predators, Sinclair emphasized that children often don't know to whom they are speaking on the Internet. "Kids might think they are chatting with a 12-year-old girl, when they are actually talking to someone who looks like this," he said.

Perhaps the biggest and most common threat to today's children, however, is their own immature and potentially life-altering poor judgments. Sinclair observed that sexting and cyber-bullying happen in even the best communities – too often with tragic consequences.

"One of the hardest parts of my job is looking parents in the eyes and telling them that I can't undo what's been done," Sinclair said. "Once that photograph or information is out there, it can't be taken back."

What You Can Do

So what's a concerned parent to do? According to Sinclair, the first step is talking to your child about potential dangers and establishing guidelines and boundaries for how, where, and when they use the Internet and any mobile devices.

"Parents need to let children know that they will be checking the computers and mobile devices they use for their protection," Sinclair said. Then, parents should follow up and actually check the devices. He suggested a variety of ways to view Internet surfing histories, including browsers' drop-down windows, "Most Visited" or "History" tabs, or the browser's cookies.

"If you can't find a browsing history, your child may be deleting the information or browsing in a 'private' window," Sinclair said. "Then it's time to have a chat."

If children are using social media Web sites that require public profiles, such as Facebook and Instagram, it's also important to lock down their account's privacy settings. Adjust any settings that allow public access to ensure personal information can only be accessed by those your child knows and trusts, Sinclair suggested.

Parents who don't want their children to have online social networking accounts should know that the law is on their side. The Children's Online Privacy Protection Act (COPPA) makes it illegal for Web sites to collect information from anyone under the age of 13. Practically speaking, this means social networking sites must remove accounts if they are notified that the account holder is under 13, Sinclair said.

OPS PARENT ACADEMY WORKSHOPS

Throughout the school year, Oradell Public School offers Parent Academy workshops that cover important topics related to students' education. Find more information and details about upcoming workshops at:

https://www.smore.com/1stw6

Knowledge is Power

When it comes to monitoring online activity, Sinclair noted that software solutions, like Spectorsoft, offer parents a way to surreptitiously surveil everything being done on personal computers, Macs, and Android mobile devices. But no dedicated monitoring software exists for iPhones, iPads, and other Apple mobile devices.

"Apple's App Store and Google's Play Store both limit these types of apps from being installed on their respective devices," explained Sinclair. "These devices don't have this type of functionality because the app stores don't allow the apps into the marketplace for download or purchase."

To complicate matters, mobile social media apps – many of them free to download – have become hotbeds for anti-social and, in some cases, criminal activities. As a result, Sinclair recommends checking phones and mobile devices for potential "problem" apps. (See sidebar on page 3 for Sinclair's Web site and app "Watch List.")

When examining phones and other mobile devices, know that app icons may be buried on different screens and in folders, or temporarily deleted only to be reinstalled. If in doubt, parents can check the device's app store or iTunes account to view a download history, Sinclair said.

Finally, parents should take advantage of the parental control tools available to make their job easier. For example, "by logging into my Internet router – the hardware that routes Internet traffic to the multitude of addressable devices in a house – I can adjust the settings to block certain Web sites or turn off Wi-Fi service at certain times of day or night for each device using its unique IP address," said Sinclair.

The key takeaway is that "knowledge is power," Sinclair continued. The technological landscape is constantly changing and what is "in" today may be obsolete six months from now. But parents can educate themselves – through school seminars and resources, by reading the newspaper, or simply by Googling technology trends – so they will be prepared as new programs, applications, and challenges arise. <OPS>

WATCH LIST

What You Need to Know About Popular Apps and Web Sites

Ask.fm: A social media Web site where users can ask other users questions anonymously, this site has featured prominently in some high-profile cyber-bullying cases.

Facebook: Once a social networking pioneer, this site is losing its appeal with youth now that parents and grandparents are using it. Still it's important to look at what kids are sharing and who they are sharing it with.

Instagram: A social networking site that allows users to share their lives with friends through a series of pictures, children run the risk of over-sharing personal information through their photos.

Kik Messenger: A free-to-download instant messenger service, Kik Messenger uses Wi-Fi instead of a cellular plan. It has more than 100 million downloads through iTunes. Think your child can't text because he or she doesn't have a cell phone? Think again.

SnapChat: This application allows users to take photos or videos, add text and drawings, and send them to others. Users set a time limit for how long recipients can view their "Snaps." After that, they are hidden from the recipient's device and deleted from SnapChat's servers... Except they're not. Recipients can permanently capture "screen shots" of messages or download apps to circumvent the SnapChat system. Beware.

Tinder: It's officially marketed as an online dating app. But a simple Google search reveals it's widely used as a "hook-up" app. Tinder gathers users' details, including Facebook profiles. Using this information along with the phone's GPS capabilities, it sends messages to potential matches and allows users to chat within the app if they mutually "like" each other's profiles.

Twitter: Twitter enables users to send and read text messages, called "tweets," that have a maximum of 140 characters.

WhatsApp: Similar to Kik Messenger, WhatsApp is a free instant messaging service that uses the Internet for communication. It allows users to text message or send images, video, audio, and their location using integrated mapping features – all without cellular service.

Whisper: This free app allows users to post anonymous "secret" messages as text overlaid on images. It is rated 17+ by Apple's App Store due in part to "Frequent/Intense Mature/Suggestive Themes."

YouTube: Using this video-sharing Web site and app, Internet users can watch videos and view user comments, which are unedited. The site recommends additional video content based on what you're watching, which can lead to some less-than-desirable suggestions. This is one to supervise with younger children.

ONLINE RESOURCES

Federal Bureau of Investigation - "A Parent's Guide to Internet Safety"

Internet Crimes Against Children Task Force Internet Safety Resources

National Crime Prevention Council's Information About Internet Safety

Bergen County Prosecutor's Office Web Site

If you have questions, comments, or new suggestions for apps and Web sites to watch, please contact the OPS Administrative Team at:

phone: 201-261-1180
e-mail:
bozios@oradellschool.org
www.oradellschool.org

Oradell Public School
350 Prospect Avenue
Oradell, NJ 07649