

Mobile App Danger – Kik Messenger

By Robert Hugh Farley, M.S.



Introduction

Recently, I presented three child abuse investigation workshops at the 27th Annual Crimes against Children Conference in Dallas where approximately 4000 child abuse professionals were in attendance. During the conference, I spoke with several law enforcement officers who were from Internet Crimes against Children (ICAC) Task Forces from around the United States. In the course of these conversations I posed the question, "What is the most dangerous cell phone or mobile device app that is used by young people today?" The overwhelming response was a mobile app that is called Kik.

Background

In the past, parents had been warned by law enforcement that in order to protect young people from Internet predators one should place the home computer in an open area such as a kitchen or family room. Today, many

young people will only use a computer or PC to complete a homework assignment or perhaps to do research for school. Today, most social contact, especially among young people, is conducted almost exclusively on smart phones and tablets. As a result, a parent's attempt to monitor his/her child's technology-facilitated social contact, can be problematic because of the many innovative apps that exist or are on the social networking horizon.

Kik Messenger or Kik was released in 2010. Kik became very popular with young people in 2013 and is an instant messaging application or app for mobile communication devices. Kik utilizes Wi-Fi or a data plan to transmit and receive text messages. Currently this free, cross-platform messaging app, which is based in Canada, is available in operating systems for iOS, Android, and Windows Phone. It is not available in a PC or computer format. In addition to texting, one can also share photos, videos, mobile webpages and other content. In 2015, Kik is reported to have recorded 200 million users.

Dangers

After downloading, Kik requires it's users to register a username. The app itself is rated 17+ and although children under 13 are prohibited from using Kik, there is no age verification process when one is registering. Unlike regular texting, users are identified only by a user name and not a real name or phone number. If a parent were to check a young person's smartphone that parent would find that all of the data is deleted when a conversation ends. Therefore, a parent who is attempting to be proactive by trying to view their child's conversations is left in the dark as previous conversations are automatically deleted. Unlike Facebook or Twitter, where you have to be "friends" or "follow"

someone before sending a message, Kik users can interact via texting at any time. As a result, Kik makes it much easier for technology-facilitated predators to operate.

Unfortunately, some young people are still unaware of the dangers of having texting conversations with technology-facilitated friends. For example, in 2014 a California man was charged federally with using Kik to blackmail and then extort eight minor females he had been "sexting" with into sending him nude photos of themselves.

As a result of the enormous amount of nude and pornographic images that were being exchanged by users of this app, in March 2015, Kik, announced that it would begin using Microsoft's PhotoDNA Cloud Service to automatically detect and report to authorities the distribution of known child pornography images.

Another dangerous feature for young people is that Kik offers its own browser with direct access to optimized webpages, using mobile web, all without leaving the Kik app. Because Kik has no parental controls, dangerous messaging webpages such as Role Play Chat or HeyHey easily allow a predator to change his personal information and then select the gender and age range of those young people he wants to text with.

Conclusion

Just banning a young person from using the Kik app is not the answer. A parent should instead sit down and talk about the dangers of texting or meeting face-to-face with those one does not really know and then discuss boundaries for the use of a mobile device such as parental permission to download apps.

Adults cannot be lulled into believing that they are attuned to today's social networking landscape. Technology continues to rapidly change. Parents, teachers and all of us who are charged with protecting children must continue our efforts to stay abreast of the many new mobile device apps that may be used by young people and child molesters who are seeking to manipulate and abuse children.