The Importance of Mobile Device App Awareness

By Robert Hugh Farley, M.S.

Introduction

Many adults are still unaware of the danger to young people who use mobile device applications (apps). According to published reports, the FBI claimed that the January 2016 murder of 13-year-old Nicole Madison Lovell, of Blacksburg, Virginia, was directly connected to her using the anonymous messaging of the Kik app with the alleged murderer who was later identified as an 18-year-old Virginia Tech freshman.

The Kik app itself is rated for children who are 17+ and claims that children under 13 are prohibited from using Kik. Yet, there is no age verification process during the registration process. Unlike regular texting, users on Kik are identified only by a user name and not a real name or phone number. Further, with Kik, all of the data is deleted when a conversation ends. Therefore, a parent, who proactively tries to view their child's smartphone conversations on Kik, is unable to see the dialogue because previous conversations are automatically deleted. With Facebook or Twitter, a user must be "friends" or "follow" someone before sending a message. Conversely, Kik users can interact via texting at any time. As a result, Kik makes it much easier for technology-facilitated child molesters to operate.

Concerns about Certain Apps

Today, social contact, especially among young people, is very frequently conducted on smartphones and tablets. As a result, a parent's attempt to monitor his or her child's technology-facilitated social contact becomes more and more challenging because there are many innovative apps currently in use, and many more are on the social networking horizon.

Anonymous social media apps such as Kik are very enticing. Apps like Kik allow young people, with little to no dating experience, to easily start connections, make friends, flirt, create relationships and in many cases communicate over the course of weeks or months without face-to-face interactions. For young people who are insecure, bored or just seeking to explore the world of social networking, apps like Kik allow these young people to project "coolness" in a variety of ways such as using a different age, a different appearance, a different persona or a different lifestyle. The anonymity may also result in the young person being far less inhibited and far less guarded than if he or she were in a face-to-face conversation.

With some apps, digital images of new social media "friends" can be hidden from parents by using one of many free photo vault apps. For example, if a parent opens the Secret Calculator Folder Free mobile app, that parent will initially see an image that looks like a simple calculator. But if one taps in a secret passcode, access is then given to a private collection of photos and videos.

Numerous mobile apps can and will track a device's location which is another danger of mobile apps. Most apps that track location will usually ask for permission first. In some cases this request appears during the app's installation and in others, the request appears the first time the app is used.

There may be legitimate reasons for some apps to require the location of the user, especially when location is essential to the purpose of the app. For instance, a navigation app such as Google Maps or Waze require the user's location in order to provide the service it offers. In contrast, social networking apps or game apps can be utilized without others knowing the user's exact location. It is important for parents to understand the apps on a young person's phone so they can distinguish these differences. Even so, there are some apps that run in the background and can track the user's location even if the user has not knowingly approved the tracking. In some cases, the only way to stop such an app from running in the background is to actually remove the app and delete it from the mobile device. It is therefore not surprising that many parents have concluded they will not grant permission for their child to use any location-required apps.

In October 2015, the California Attorney General's office published an information tip sheet titled, Location, Location, Location: Tips on Controlling Mobile Tracking (Consumer Information Sheet 18).

The key advice in the tip sheet is the instructional information on how a parent can disable the mobile tracking feature on Android and iOS (iPhone and iPad) devices. The tip-sheet also includes location-sharing advice for mobile versions of Gmail, Yahoo and Outlook email.

Conclusion

Simply banning a young person from using social media apps may no longer be a realistic solution as apps are clearly not a passing phenomenon. A discussion by parents with their children on boundaries and limits when using a mobile device is essential. Parental permission for the download of each app on a mobile device, and retaining the password, should certainly be considered. Parents need to express interest in apps and learn the purpose of each and every app on their child's mobile device. In addition, parents must regularly follow up and continue to have conversations with their children about the dangers of social media, texting or meeting face-to-face with "friends" they've only met online or through apps.

Remember that the social networking landscape is constantly changing and technology is rapidly evolving. Adults cannot be complacent. 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 could be used by young people and child molesters who are seeking to manipulate and abuse our children.