Mobile Device Dangers: Snapchat, Snap Map and Caller ID Spoofing

By Robert Hugh Farley, MS

Introduction

A mobile application, known simply as an "**app,"** is a software application or a computer program that is designed to run on a mobile communication device such as a phone, tablet or watch. Today, most mobile communication devices are sold with several apps bundled as pre-installed software, such as a web browser, an email provider and a calendar. With the ever-growing number of apps available at the Apple iOS or the Android App stores, adults and young people are downloading more and more apps to their mobile devices.

For many, who are responsible and take safety precautions, some of the very popular social networking and messaging apps can be an easy and fun way to meet people and stay in touch with friends. Unfortunately, many are unaware of the dangers for children and young people who utilize these social apps because children and young people can be exposed to not only graphic images but in some cases, child molesters.

Snapchat and Snap Map Background

Snapchat, first released in 2011, is a popular social networking app that lets its users easily snap (take) and exchange photos, videos and text messages with a selected group of friends. As of October 2019, Snapchat reports having 210 million daily active users.[1]

Unlike *Facebook* or *Twitter*, which memorializes everything a user posts, the photos and videos that are shared on Snapchat are meant to disappear once they have been viewed or within a pre-designated time. Unfortunately, many children and young people fail to realize that like anything that is shared online, the digital images are often still there, in some form, somewhere, forever.

Like other social media apps, Snapchat is extremely easy to download and use, despite easily overcome age restrictions. For example, once the Snapchat App has been downloaded to a device, all that one needs to sign up is a name, email address and a birthdate. According to Snapchat's terms of service, a user must be 13 years old to join. But, Snapchat unfortunately has no real age-verification process, so it is extremely easy for one to falsify their age by simply providing a fake birthdate.

[1] Snapchat daily active users 2019 - Statistic. www.Statista.com

After providing a birthdate (real or fake), one next selects a "user name" or profile display name to connect with friends or discover new friends. Many users will also use a **Bitmoji** for their profile image**,** which is a personal, animated cartoon avatar (created using another app). Once one has created an account, Snapchat offers a variety of features, allowing one to modify photos or make funny enhancements. Another feature simplifies video chatting or conferencing. Snapchat also offers users entertainment news and games.

Unfortunately, as a result of the inadequate age-verification process, children and young people who have joined can be easily manipulated by their new adult Snapchat "friends." Some of the new "friends" will snap sexually explicit photos to vulnerable victims and will groom vulnerable youth to send the sexually explicit pictures of themselves, commonly known as selfies. They might obtain more images from youth by saying that the photos will quickly disappear per the app's functionality, which lowers the child's inhibitions.

Snap Map, first released in June 2017, is a Snapchat add-on feature that displays a user's location on a map in real time. Snap Map uses geo-location to track a user's mobile device. As a result, Snap Map friends will see an image or Bitmoji on a map. Further, it lets friends see where a person is located, right down to the very street. The geo-location updates every time the app is opened, not just when a photo, video or text is sent or snapped. If friends have opted into Snap Map, their locations are visible, too. One can turn this feature off, or use it in Ghost Mode, which allows the user to view the map but not be seen by others.

Prevention

The biggest risk for a child or young person using any location-based app like Snap Map is having their location seen by all of their friends, because some Snapchat acquaintances may not be real friends and may have bad intentions. It is frightening to think that a molester could stalk a child or young person in real time from home, school, a store or even to church. It is strongly encouraged that if children or young people are going to use Snap Map, that it only be used in the Ghost Mode. Even better, that it not be used at all. Keep in mind that other elements in the background of photos can also reveal locations (such as the image of a school, store, sign, neighborhood, car, etc.), even if the Snap Map add-on of this app, or any similar app, isn't utilized.

Caller ID Spoofing

Caller ID, or caller identification, while seemingly innocuous, is another technology that may be used in an alarming manner. As background, the caller ID process is initially transmitted at the start of the phone call and identifies the incoming caller before the receiver answers the phone. Call "screening" is the process of evaluating a telephone call before deciding whether to answer the call or not. Anyone who has a cell phone can screen a call—call screening is typically

done by checking the receiver's caller ID display to see who or where the call is coming from. Unfortunately, with newer technology, the caller ID information that is received on the device can be falsified.

Caller ID "spoofing," or faking, is a technology that allows one to alter the information sent to a device's caller ID display in order to hide the caller's true origin. In simpler terms, caller ID spoofing allows one to display a phone number different than the actual number from which the phone call was placed. Multiple "caller ID faker" apps are available for download at the Apple iOS or the Android App stores. These apps, some of which are free, are advertised in the App stores as a funny way to prank or fool your friends. Other faker apps that are available at the App stores will even allow a text user to spoof or fake the mobile number that was used in connection with transmitting a text message.

Prevention

Children and young people who use social networking and messaging apps are often very trusting regarding the people or "friends" that they have met or communicated with online. As part of the grooming process, a child molester will progress (sometimes very quickly) from just messaging, and will attempt to actually talk in real time with a vulnerable child or young person. When receiving a call, a child or young person would typically check their phone's caller ID display to see who or where the call is coming from, giving them a sense of security. Caller ID spoofing apps present an enormous danger for these children and young people because it allows the molester to not only fake an identity, but also fake a mobile phone number.

Conclusion

Technology continues to rapidly change. All of us who are charged with protecting children must continue our efforts to stay abreast of the many new devices, software programs and the latest apps that may be used by young people, as well as people seeking to manipulate and sexually abuse children.