How to protect your children

Cell-provider based services*

- The major cellular service providers have programs to help parents monitor their children's activity on their mobile devices.
- Programs are integrated into the phone's operating system and administered by the provider.
- Some features can include: setting restrictions on times the device can be used and who can be contacted, receiving alerts on activity, tracking location of the device, blocking web content, monitoring downloading of apps, providing protection from spyware/malware, and restricting activity while driving.

**Each provider's abilities and fees are different and are updated frequently. Check with your provider about which features would work for your family.*

Third-party apps**

- Some third party applications go further in monitoring user-created data, such as social media posts, pictures, and instant messaging, which most cell provider based security applications are incapable of monitoring.
- Most third-party applications are significantly more expensive and some may be easily bypassed by a "tech-savvy" child.
- Some features can include: recording keystrokes, recording an activity log, providing access to photo and video galleries, blocking and monitoring of web content, allowing remote access to mobile device's settings.

***iKeyMonitor and Mspy are a few examples. Programs are created and developed frequently.*

Parents: Stay Involved

- Remember that cell phone providers' capabilities are ever-changing.
  - ♦ Talk to your provider about what works best for you and your family.
- Third party applications and cell provider-based services cannot be a substitute for talking to your children about online safety and for checking up on their internet use yourself.
- Encourage teens to be themselves online; do not post or become part of conversations that will get them in trouble or negatively impact their future.
- Encourage your teenager to feel comfortable talking to you or another trusted adult about content that confuses or upsets them.
- Discuss the importance of reporting to a trusted adult any threat of violence to another individual, regardless of whether the threat appears to be a joke.
- Talk about the dangers of disclosing personal information to strangers.
- Monitor, monitor, monitor!

City of Virginia Beach
A Community for a Lifetime

Office of the Commonwealth's Attorney
2425 Nimmo Parkway, Building 10B, 2nd Floor
Virginia Beach, VA 23456
757-385-4401
Facebook: www.facebook.com/ColinStolle1
Twitter: @ColinStolle
www.vbgov.com
ocaadmin@vbgov.com

Always Online:
Are your children safe from online predators?

Colin Stolle
Commonwealth's Attorney

A look at social media use and a guide for parents to monitoring their children's activities, provided by the Virginia Beach Office of the Commonwealth's Attorney

Created: May 2016

Dangers of Social Media Use

- In **82%** of online crimes against children, the offender used the victims' social networking sites to gain information about their interests, home and school information, or their whereabouts at a specific time. *(Journal of Adolescent Health 47, 2010)*
- **Over half** of children sexually solicited online were asked to send a picture to the offender. *(Wolak, Mitchell and Finkelhor. Online Victimization of Youth: Five Years Later. Alexandria, VA. National Center for Missing and Exploited Children. 2006)*
- Approx. **14%** of high school students have accepted an invitation to meet an online stranger or invited the stranger to meet them. *(Rochester Institute for Technology, 2008)*

Most social media apps can be fun and safe, unless they're in the hands of a predator or an unsuspecting child or parent. Some common risky behaviors include:

- **Oversharing of info**- Such as home address, school, age, and phone number. Giving this information can be dangerous and may be made public to anyone who visits a user's profile page. Even if account settings are set to private, users can be at risk.
- **Imposters**- Social networking sites make it very easy to pretend to be someone else.
- **Location-based services**– These expose the profile user's location. The services also have a feature that allows users to tag who they are with at any given time. Sharing location information can potentially put users at risk of being robbed, sexually assaulted, or worse. Predators can use this tool to track users' movements and determine when users are alone or not at home.
- **Posting photos**- One of the features of online social networking that many teens enjoy is the photo-sharing feature. This feature allows users to post photos 24 hours a day from computers or mobile devices. The Internet makes it easy to obtain photos and use the images in any way a predator may choose, including identifying or exploiting victims.

Keeping Up with Technology

Children and adolescents use mobile devices (including cell phones and tablets) as well as stationary computers and laptops to access the internet, making their activities difficult to monitor. Ever-changing technology makes it hard for parents to stay ahead of their children's attempts to bypass parental controls. The only way to truly protect your children is to stay involved, every day, with their online activity.

Social Media Apps

Every day, social media apps are released that:

- keep content only temporarily
- make users anonymous
- reach unintended audiences

Many social media apps can have unintended consequences when not used and monitored appropriately.

The following is a list of apps that are currently popular with teenagers and should be monitored regularly by parents. This list was compiled in May 2016 based upon a review of cases handled by the Commonwealth's Attorney's Office, investigation by law enforcement, and additional research. Please keep in mind that apps are constantly being created, developed, and improved.

- **Kik**—Allows user to send texts, pictures, and video. Users can be anonymous and talk with strangers. Users can also surf the web from within the app.
- **Snapchat**—Lets users put a time limit on the pictures and videos they send before they disappear. Teens believe images go away forever; that is not true. Anything posted online never truly "goes away."
- **Whisper**—A "confessional" app that allows users to post anything on their minds without repercussions. "Whispers" can go public unintentionally and the content can be inappropriate for teenage users.
- **Ask.fm**—Allows users to ask and answer questions posted by others. It can be anonymous, which can result in teenagers exhibiting behavior they otherwise wouldn't.
- **Yik Yak**—Geographically based anonymous chat app that allows users to send photos and texts to people near their location.
- **Tinder**—Mainly used as a dating tool or anonymous hook-up locator by adults; helps people find others in their geographic location for chatting and photo-sharing.
- **Omegle**—An anonymous chat app that allows users to discuss anything they like. Users get paired up with strangers to chat.
- **Calculator Vault**—Looks like a regular smartphone calculator, but is a secret way to hide photos, video, and information. The user can take photos from within the app. It is password protected.
- **Burn Note**—A messaging app that erases messages after a set period of time. Teens may reveal more than they normally would since messages are "deleted."
- **Line**—A text, video, and voice-messaging app that includes group chats and games. Texting and video calls are free (even internationally).