SECOND EDITION

PARENTING IN THE DIGITAL WORLD

A STEP-BY-STEP GUIDE TO INTERNET SAFETY

CLAYTON CRANFORD

PARENTING IN THE DIGITAL WORLD

A STEP-BY-STEP GUIDE TO INTERNET SAFETY

SECOND EDITION

Author Clayton Cranford, M.A.

ISBN 978-1974552542

Dedicated to My Family

The Cyber Safety Cop program, my work fighting human trafficking, and this book would simply not be possible without the love, patience, generosity, and help from my family. This book is dedicated to them:

To my indomitable wife, Gretchen, who has given me constant and unwavering support, our two boys, Clay and Zachary, who love technology and are my “goofballs,” now and forever.

To my parents, Otis and Patricia who taught me to do good in the world, serve others, and be true to myself. To my two older brothers, Michael and Matthew, who introduced me to computers and technology when the Commodore 64 was state of the art. And my sister Kimberly, who’s memory is a sweet presence in my life everyday.

And finally, this book is also dedicated to the parents, teachers, principals, law enforcement officers, and counselors who are dedicating themselves everyday to keeping our children safe. Thank you.

Contents

Preface

Thank you for purchasing the second edition to my book, Parenting in the Digital World. It has been two years since I published the first edition, and since that time there have been many new developments in technology. There are new devices, new operating systems, but at the same time a lot has not changed. Parents, educators, and law enforcement are still inundated with incidents of online sexual exploitation, threats, harassment, bullying, self-harm, and suicide. In addition to new apps and devices included in this second edition, I will help guide you through critical discussions every parent must have with their child about pornography and threatening behavior. Technology is a moving target, and we must always be aware of the new and evolving challenges our children are facing.

Speaking with an elementary school principal after I finished a Cyber Safety Workshop for her 150 5th graders, she remarked how important this education is for her students, and how disappointed she was at the lackluster turnout for the parent workshop I did the prior week.

An unfiltered, unsupervised internet is one of the most dangerous places for our children to be.

“Every parent of every child in your class should have been there last week,” she exclaimed.

We only had about 25 parents show up to the well-publicized workshop. This kind of turnout is not unusual. If by sheer coincidence, there had been a cyberbullying incident at the school just before my workshop, we would have had a packed room. The parents who do attend the workshop are blown away by what I show them and insist we schedule another workshop next month so they can get the word out. They can think of ten parents who needed to be at my seminar. The second class is always better attended. Parents are tired and overworked. I should know. I am a parent of two teenaged boys. After investigating thousands of cyber-related crimes and other incidents, I have gained a perspective that most parents do not have: An unfiltered, unsupervised internet is one of the most dangerous places for our children to be. Why aren’t parents attending a free class that will help make the Internet and social media a safer place for their children? After talking to thousands of parents who have attended my seminar, I have discovered many parents are living under false assumptions about their child’s digital world.

The purpose of Parenting in the Digital World is to bring you up to speed about the potential threats your children may face when they connect to the Internet and abolish the three primary false assumptions parents have about their child’s online safety.

False Assumption #1

It is not that big of a deal. The National Crime Prevention Council reported that more than 80 percent of students surveyed said they either do not have set boundaries from their parents about what they can do online, or know how to get around restrictions easily. Nearly 100 percent of parents I talk to after I

learned about an issue with their child's online activity had no idea what was going on in their child's online world. They gave their teen or tween a smart phone with no parental controls or restrictions. They are flabbergasted to find their child had created multiple social media accounts, was a victim or perpetrator of cyberbullying, viewing pornography, interacting with adult strangers, or had sent nude images of themselves to others. There is too much at stake not to be engaged in our children's digital world.

False Assumption #2

I**f my child was having a problem online, they would tell me.** In a report from the Cyber Bullying Research Center (2016), only 1 in 10 children will tell a parent if they are the victim of cyber abuse. Why does only 1 in 10 teens feel comfortable enough to tell their parents about being a victim of cyberbullying? The answer is simple: They are afraid of losing their phone or access to their social networks. Teens would rather suffer through being bullied than lose their vital connection to all their friends. How can we turn that statistic around? We need to make children feel safe to come to us and tell us about problems they encounter online.

False Assumption #3

This technology thing is too much for me; I'll never understand it. Parents are busy working, getting their kids to and from sporting events, and putting a hot meal on the table. The thought of having to take on one more task, as daunting as learning how to operate their child's electronics, makes them want to throw their hands in the air and surrender. The bad news: If you care about your child's safety, you must learn a thing or two about your child's electronic devices. The good news: I wrote this book, Parenting in the Digital World, for you. You don't have time to read 200 plus pages about bullying research or scour the Internet on how to set up parental controls on your child's numerous devices. I have done it for you. Even if you know nothing about computers or mobile devices, this book will walk you step-by-step through each of your child's mobile devices, computers, and game consoles, and show you how to turn on the obscure parental controls that will help keep your child safe.

If you are reading this book, then I don't have to convince you that there are online threats and your child is vulnerable. You want to know how to talk to your child about your concerns and understand how all their technology works. You have taken the first step. It may seem scary, but it is worth it. This book will help you the rest of the way.

Introduction

On a bright, sunny first day of school, I walked through the front doors of my middle school and was immediately greeted by the office manager.

“Deputy Cranford, thank goodness you are here!”

Those words and their urgency were not what I wanted to hear walking through the door of my new job as a School Resource Officer. I found Jessica, a 7th grade student, sitting in the counseling office, doubled over in a chair weeping uncontrollably. The school guidance counselor, with a look of sadness and concern, sat next to her rubbing her back, trying to calm the distraught twelve-year-old girl.

Through the tears, Jessica told me that over the summer her boyfriend had asked her to send him a nude picture of herself, which is known among students as “sexting.” She didn’t want to do it, but he pestered her relentlessly until she did. After recounting her story, she framed her torso by placing one hand below her chin, and the other at her waistline and said, “I sent him this.”

Jessica and the boy she sent the image to were no longer “dating.” She believed that he had sent the image to at least one other boy, his close friend. After hours of investigation and interviewing Jessica’s ex-boyfriend and his friend, I was able to delete the image from his phone. He promised he had not sent the image to anyone. His friend had seen the image, but it had not been sent to him by text or email.

What could I tell Jessica and her mother? I could not guarantee that the image was truly gone. The sad truth of the matter was once Jessica sent that nude image of herself to her boyfriend, it was completely out of her control. Her boyfriend could have sent that image to one friend, or fifty. Only time would tell.

What advice could I give them? “Don’t do that again,” wasn’t going to cut it. There had to be more. There had to be a way for Jessica’s mother to supervise her daughter's online activities adequately, and for Jessica to learn how to navigate cyber space safely.

That experience and hundreds thereafter formed the Cyber Safety Cop program. I created the Cyber Safety Cop program to teach parents and students how to be safe online with all forms of social media.

The goal of this book and the Cyber Safety Cop Workshops are one in the same: Parents will gain an understanding of how important social media and social networking are to their children. They will understand the unique threats that exist online, including cyberbullying, impersonation, identity theft, sexting, sexual predators, human trafficking, digital reputation management, pornography, and other high-risk behaviors.

Most importantly, parents will be given tools and resources to help them properly supervise their children online. They will walk away with a strategy that include: guidelines to be implemented in their home that will immediately make their children more cyber safe.

Students will learn about privacy and why controlling who has access to their social networks is key to a safe and enjoyable experience online. They will, maybe for the first time, come to understand what their digital reputation is and why establishing a good, or bad one, can have lifelong consequences. Finally, they will learn how to deal with bullies and other negative behavior when it inevitably comes their way.

I promise you what I promise every parent or student who attends one of my Cyber Safety Cop Workshops: You will put down this book empowered.

The threats are real and sometimes disquieting, as thousands of teens like Jessica can attest, but by the end of this book, you will have a plan. And something else really special will happen too. You will have amazing conversations with your child about something that is intimately important to them—technology and social media. You will have a window into your child's world. You will see things in your child's social network that will give you amazing insight into what is important to them. Some of it may cause pause, and some of it will affirm what you already know. Either way, it will help you draw closer to your child.

The Cyber Safety Cop Plan

EDUCATE YOURSELF

- Go to a Cyber Safety Cop Parent Seminar (Page 95)
- Subscribe to the Cyber Safety Cop Newsletter (www.CyberSafetyCop.com)
- Review games and apps before you download them for your child at www.commonsensemedia.org

TALK WITH YOUR CHILD

- Use Internet Usage Contract (Page 37)
- Talk about your safety concerns
- Be open and direct

USE PARENTAL CONTROLS

- Follow the directions in this guide to activate the safety settings in your operating systems, search engines, and games
- Setup website filtering on your home network using www.opendns.com

SET RULES AND EXPECTATIONS

- Respect age limits on social media (Page 45)
- Enforce consequences when appropriate
- Charge your child's devices in your room at night

ACCOUNTABILITY

- Know all of your child's user names and passwords to all of their accounts
- Log into your child's social media accounts as them to monitor activity
- Periodically physically review the content on your child's device
- Install a monitoring/filtering application on your child's device

CREATE BALANCE

- Establish "screen time" limits for school nights and for weekends (Page 12)
- Plan family time without electronics
- Curb your own bad digital habits

Social Media Defined

When you think of social media, I am willing to guess that Facebook and Instagram first come to mind. If we only look at Facebook and Instagram, two of the most popular social media platforms in the world, we will draw too narrow a definition and miss all the other places children communicate.

A broader, more inclusive definition of social media should be:

> Social Media is any device or application that allows a user to communicate with another person.

This new definition of social media will hopefully open your eyes to a much bigger world. These devices and applications are really just portals to other people. The portal may be a web cam chat room with strangers or something as innocuous as Words with Friends. For parents to properly monitor their children's social networks, they must first realize that social media does not only exist on smart phones, tablets, and computers but exists in a whole new world of social networking that is constantly being created and expanded.

The Problem with Social Media

Social media and socially embedded technology are moving targets. Today's hot social media app could be easily replaced tomorrow with a new competitor.

After investigating cyberbullying and other social media related crimes over the years, I have traced the root of all the threats on social networks to two basic problems inherent in nearly all social media platforms.

1. Children can communicate and meet people outside their parent's sphere of influence and control.
2. Children and adults can communicate anonymously without any accountability, removing the natural inhibition or fear of getting caught.

Today's teens are sitting in their rooms with mobile devices in their hands. They have the Internet and social media access literally at their fingertips. Our social media connected teen is

sharing intimate details with potentially 3.5 billion people on the Internet.[1] An unsupervised, unfiltered Internet will leave a child open and vulnerable to threats and attacks that the parent and child are completely unprepared for.

Now that you understand what the two basic problems with social media are, you will look at the Internet in a new and completely different way. You will quickly see how a social network's privacy setting, or lack thereof, can allow strangers into your child's life. New social media applications are being created daily. Developers are looking for the next big thing. They are pushing the boundaries. They are trying to entice teens by creating new and exciting online experiences. Often, these new, exciting environments are not safe.

Action Plan

- Take an inventory of all the electronic items in your home or child's life and how they connect to the Internet (e.g., Wi-Fi, hardline, cellular, or a combination)?
- Do your child's devices have parental controls?
- Can your child communicate with another person with this device? How do they communicate (e.g. Text, camera, or voice)?
- Are the people they communicate with a defined group of people that you know, (i.e. private server for Minecraft for just friends), or strangers?
- Can you filter or block the device's ability to communicate with others? For example, some games allow you to turn the chat feature off, or you can unplug the microphone to disable the voice-over-IP chat?

Notes

1. Internet Users. (n.d.). Retrieved August 9, 2017, from http://www.internetlivestats.com/internet-users/

YouTube Safe Search Desktop

To filter out adult and inappropriate content on YouTube, “safe search” settings must be put on every browser and YouTube app, on computers and mobile devices. Launch a browser window and type www.youtube.com in the web address bar.

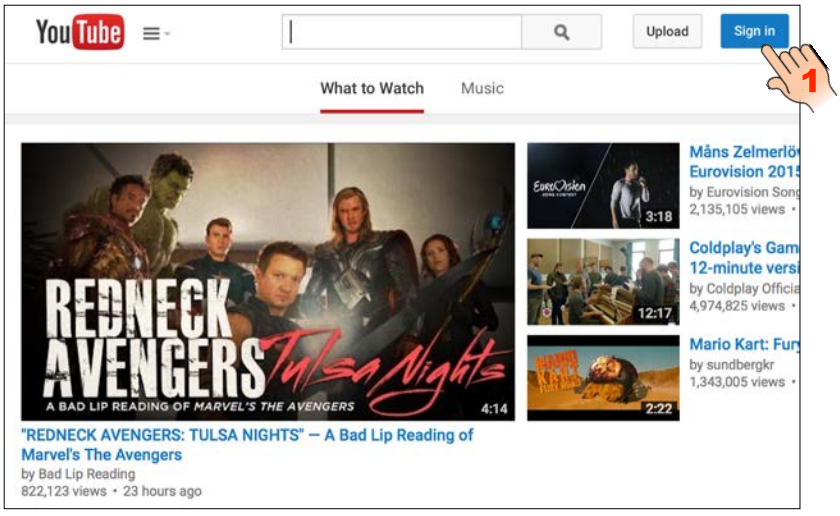
1. Click the blue **Sign In** button in the top right corner of the screen and follow the prompts to sign in.

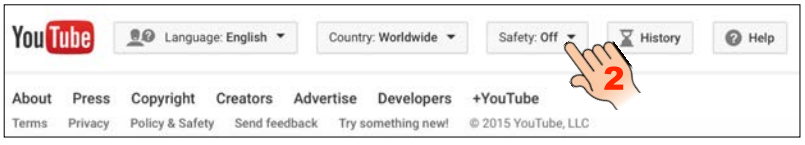
2. Once YouTube loads, Scroll down to the bottom of the page and click the **Restricted Mode** button.

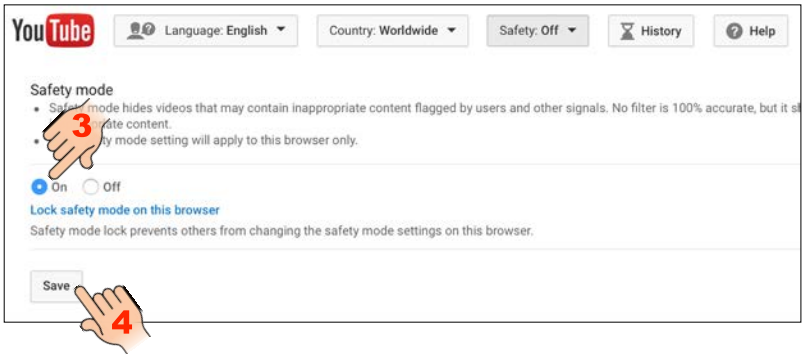
3. Click **On**

4. Click the **Save** button. To lock these changes so no one can change them without your password, click “Lock safety mode on this browser.” You’ll be prompted to enter your password. Once that information is entered, the feature is locked and can only be unlocked by entering your password again.

   You’ll know the parental controls are activated when you do a search. Stated at the top of the search results will be the phrase “Some results have been removed because Safety mode is enabled.” You need to do this for any and all browsers on your computer that you think your child might use to access YouTube. The process is the same.







About the Author

CLAYTON CRANFORD IS

The Cyber Safety Cop

Clayton Cranford is a law enforcement professional based in Southern California and owner of Total Safety Solutions. Clayton is one of the nation's leading law enforcement educators on social media and child safety. He created Cyber Safety Cop, an Internet and social media safety program. It teaches parents and students how to avoid the inherent risks of social media and other web based platforms by using safe habits.

Clayton has more than 20 years of teaching experience and has been a featured speaker at the National Conference on Bullying, the Southwest Conference on Human Trafficking, the California Association of Crime Prevention Officers, and the National Association of School Resource Officers.

Clayton was awarded the 2015 National Bullying Prevention Award from the School Safety Advocacy Council, and the 2015 American Legion Medal of Merit for his bullying prevention work.

Clayton was also a member of Orange County, California's school threat assessment team. He has investigated threats, weapon possession, in nearly 200 schools. Clayton also teaches threat assessment investigation to law enforcement agencies through out the United States.

Clayton has partnered with Agape International Missions (AIM), a leader in the fight against child sex trafficking in Cambodia. Clayton has served overseas with AIM in Cambodia's child sex trafficking epicenter and speaks at various Human Trafficking symposiums and conferences.

Clayton is married with two boys who love the Internet and technology. Clayton has a Bachelor's Degree in Philosophy and a Master's Degree in Criminal Justice.

PARENTING IN THE DIGITAL WORLD

A STEP-BY-STEP GUIDE TO INTERNET SAFETY

SECOND EDITION

"Parenting in the Digital World is brilliantly organized, easy to follow, and offers screen shots and step-by-step instructions on how to manage the privacy settings on different operating systems and applications. Knowledge is power and I am delighted to recommend this empowering book! Together, we can stop crimes against children. Be Brave."
—Erin Runnion, Founder of The Joyful Child Foundation

"This book answers the number one question parents of digital kids have today, "How Can I Keep My Child Safe Online?" Parenting in a Digital World is an indispensable guide that should live on the nightstand of every parent raising kids today."
—Diana Graber, Co-Founder, Cyberwise.org and Founder, CyberCivics.com

Parenting in the Digital World is an up-to-date guide containing all of the essential information parents need to create a safe environment for their children online.

Cyber Safety Cop's founder, Clayton Cranford, will take you step-by-step through the hidden settings on all the most popular social media apps, operating systems, gaming consoles, and mobile devices.

Clayton Cranford is a law enforcement professional based in Southern California. Clayton's experience as a juvenile investigator, school resource officer, threat assessor, and father of two teenaged boys has made him one of the nation's leading law enforcement educators on social media and child safety.

Clayton has taken his extensive experience and created this manual for parents to address key safety issues in their child's digital lives.

The second edition includes updated parental control guides on all the devices your child is using, and new chapters on critical online safety issues: How to talk to your child about pornography, threats and consequences, how to protect yourself from being hacked, and how to create a culture of safety and accountability in your home.