Most people think that being careful with your online activity, limiting online accounts, creating strong passwords and having antivirus installed will keep you from becoming a victim of internet crimes; unfortunately, it won't. By reading this guide, you will learn what precautions you can take that will help keep you, your job, your family and your finances safe from cybercrime.

The Internet welcomes iPredators into our homes without an invite. https://www.ipredator.co defines iPredator as: cyberstalker, cyber harasser, cybercriminal, online sexual predator, internet troll, cyber terrorist, cyberbully, online child pornography consumer/distributor or engaged in internet defamation or nefarious online deception. iPredators exploit, victimize, coerce, stalk, steal, etc. from anyone, any age, any sex, and any religion.

iPredators use many different strategies in order to gain access to your computer. For example, they may send you an email or text message that, once opened, will install malware on the device. Once the malware is installed, the perpetrator will have complete control of the computer, they can open the camera, use the microphone, track your location, and record all passwords and conversations that take place.

iPredators are not the only problem we face. Without parental controls, children risk being exposed to content that has intense violence, blood and gore, and strong sexual content. Brad Bushman, a communications and psychology professor at Ohio State University, claims to have evidence that violent video games can lead to "an increase in aggressive thoughts, angry feelings, physiological arousal, including increased heart rate, and aggressive behavior. They also decrease helping behavior and feelings of empathy for others."

Last, but not least, for marketing reasons, many internet service providers track browser history and sell it to marketing companies. Social media is used to collect personal and private information and used to feed consumers advertisements. What does all of this mean? With our data being exploited, we are opening the door for criminals to come in and take advantage of our family, our life, our credit, our money, our reputation, and our stability.

It is in our nature to protect ourselves and our children from potentially dangerous situations, which is why most parents, at some point, have taught their child, "do not talk to strangers." What about online strangers? After visiting 2 counties, over 18 schools, and several thousand students in Alabama, from grade 3 up to college level and having in-depth conversations, I have learned that most have one thing in common … they feel the "stranger danger" rule does not apply to online strangers. Many students believe strangers can cause harm in person, but not online.

The false sense of security the internet is providing has become a dangerous problem for people of all ages, not just kids. By entering one small piece of information (ex: name, email, username or even a photo) into a people search site, every detail from your residential history to the type of lifestyle you live can be seen. Everytime you go online, you leave behind digital footprints. The more social media accounts you have, the easier it will be to find out who you are, where you are, who your friends are, and even who your family is.

Blackmail and Sextorion

According to www.enough.org, 92% of child pornography comes from 5 countries in the world … the United States ranks #2. http://www.missingkids.com/home shows there is 747,408 registered sex offenders in the United States, with over 100,000 sex offenders being lost in the system. In 2018, 424,066 reports of missing children made it to law enforcement. There are thousands of perpetrators that are online looking for their next victim.

For More internet statistics involving children/teens and the internet click here

According to https://www.brookings.edu/research/sextortion-cybersecurity-teenagers-and-remote-sexual-assault/amp/, a few of the many predators that have been sentenced for Sextortion and remote sexual assault against teenagers, are:

Louis Mijangos
Louis used trojan emails and instant messages embedded with malicious software that would give him complete access to the victim's computer. Louis had over 15,000 videos, 900 audio clips, and 13,000 screen captures. He had access to over 129 computers and 230 victims. 44 victims were minors.

Jared James Abrahams
Took control of the victim's computer by installing malware, used keylogger to record computer activity, and took photos of the victim using their own camera. He would then contact the victim and make threats. Police found that Jared had 12 young female victims and control of 100-150 computers.

Ivory Dickerson and Lucas Chansoler
3,800 victims were being exploited by a civil engineer and British military contractor. Ivory and Lucas used malware called bitfrost in order to gain control over computers.

Michael Ford
Worked at the U.S. Embassy in London. He used phishing via emails in order to pretend to be a part of “Google's account deletion team.” Michael had 75 victims and over 450 complaints.

https://www.brookings.edu/research/sextortion-cybersecurity-teenagers-and-remote-sexual-assault/amp/

How Predators Find Victims:

Predators will create several fake social media accounts, search for a target that seems vulnerable, and make contact. For example: a 13 year old female with a social media account, no parental controls, and no privacy settings just posted about her missing dog. Through studying the victim, he learns that the girl is upset about her missing dog. The predator contacts the victim expressing concern while pretending to be a 14 year old attractive male. This initiates a conversation and after a short time, trust is built.

At this point, the predator has several options.

1. He can send a message that contains a virus which would allow the predator to have complete access to the victim's computer.
2. Request the female to do a cam session with her and eventually talk her into exposing herself. This will later become a case of sextortion.
3. Request her phone number, send a link via text that contains a virus, and will allow him complete control of her device once she clicks it.
4. With the information he already has, he can use a people search engine to find out where the girl lives, who her friends and family are, how much money her family makes, and more. This could lead to blackmail, exploitation, fraud, impersonation, kidnapping, sex and or human trafficking etc.
5. Grooming: please see https://internetsafety101.org/grooming for the complete definition.

Why Be a Concerned Parent?

An epidemic that is affecting children of all ages, and although rare, can have an end result of death. What is it and how can you take precautions?

Before the internet existed in everyone's home, being bullied was limited to a face-to-face encounter or over the phone. Thanks to social media, bullying doesn't stop at the school or playground, anymore. The harassment follows you. Safe spaces do not exist. Someone who habitually dominates, acts aggressively, and/or abuses others is known as a bully. A bully can be a sextortionist, cyberstalker, cyber harasser, internet troll, and/or a cyberbully.

There are no laws against bullying another person; however, it is illegal to harass another person. Each state sets its own standards and laws when dealing with harassment.
To find out what your state laws are please visit https://www.stopbullying.gov/laws/index.html

According to MottPoll.org in 2010, bullying was rated #6 of the top health concerns for children. As of 2017, it is now considered parents #1 concern. Why is bullying such a fast growing concern? https://www.psychologytoday.com states, “Bullying causes stress and anxiety. When someone is stressed, there is a stress hormone called cortisol that becomes elevated. Research shows chronic elevated levels of cortisol during childhood impairs cognitive development and negatively affects the immune system.”

If you want to know more information about long term effects please visit: http://www.brainfacts.org/Thinking-Sensing-and-Behaving/Childhood-and-Adolescence/2015/Bullying-and-the-Brain.

Laws Protecting Children Online:

The Children's Internet Protection Act (CIPA) was enacted by Congress in 2000 to address concerns about children's access to obscene or harmful content over the Internet. CIPA imposes certain requirements on schools or libraries that receive discounts for internet access or internal connections through the E-rate program – a program that makes certain communications services and products more affordable for eligible schools and libraries. In early 2001, the FCC issued rules implementing CIPA and provided updates to those rules in 2011.

Schools and libraries subject to CIPA may not receive the discounts offered by the E-rate program unless they certify that they have an internet safety policy that includes technology protection measures. The protection measures must block or filter internet access to pictures that are: (a) obscene; (b) child pornography; or (c) harmful to minors (for computers that are accessed by minors). Before adopting this internet safety policy, schools, and libraries must provide reasonable notice and hold at least one public hearing or meeting to address the proposal.

https://www.fcc.gov/consumers/guides/childrens-internet-protection-act

Children’s Online Privacy Protection Act (COPPA):

This Act directed the Commission to set forth limited rules governing the online collection of personal information from children 12 and under by commercial websites that maintain personal information, as well as other websites that have actual knowledge that they are collecting or maintaining personal information from a child 12 and under. Principally, COPPA requires website operators to:

1. Post a privacy policy on the website.
2. Provide notice directly to parents.
3. Get parental consent.
4. Allow parents to review personal information collected from their children.
5. Allow parents to revoke their consent, and delete information collected from their children at the parents’ request.
6. Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of children’s personal information. Not condition a child’s participation in certain activities on collection of more personal information than is reasonably necessary.

https://www.ftc.gov/sites/default/files/documents/rules/children%E2%80%99s-online-privacy-protection-rule-coppa/coppasurvey.pdf

**The Federal Trade Commission has provided an easy to read chart on the six step compliance, which can be found by clicking on the link below.

https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance#chart

Neighborhood Internet Protection Act (NCIPA):

To require schools and libraries receiving universal service assistance to install systems or implement policies for blocking or filtering internet access to matter inappropriate for minors, to require a study of available internet blocking or filtering software, and for other purposes.
In general -- no services may be provided under subsection (h)(1)(B) to any elementary or secondary school, or any library, unless it provides the certification required by paragraph (2) to the commission or its designee.

For more information, please see: https://www.congress.gov/bill/106th-congress/senate-bill/1545/text

The Family Educational Rights and Privacy Act (FERPA) *(20 U.S.C. § 1232g; 34 CFR Part 99)*:

A federal law passed in 1974 that bars the disclosure of personally identifiable data in student records to third parties without parental consent.

The Protection of Pupil Rights Amendment (PPRA) (20 U.S.C. § 1232h; 34 CFR Part 98):

Was enacted in 1978 and applies to student surveys, instructional materials or evaluations funded by the federal government that deal with highly sensitive issues.

You can find more information about FERPA and PPRA at
https://www.studentprivacymatters.org/ferpa_ppra_coppa/

Help for Parents:

If you are a parent of a child age 13 and younger, you can rely on FERPA, COPPA, PPRA, CIPA. If your child is above the age of 13, you are on your own. This is where This guide will provide tips, resources, and guidance so that you know you are doing everything you can to protect your family. .

Parental controls are a must. There are many ways you can set up parental controls:

1. Most routers that you purchase do not come with built in parental controls. However, you can go to open DNS and set up parental controls on any router. Some routers have apps that will allow you to easily set up parental controls and even pause certain users.

2. Purchase a device or app extension to connect to the router. A good example of this would be Circle by Disney. Circle will allow you to customise the on and off time per user, websites allowed, and choose whether or not they can use a VPN and much more.
3. Most devices will allow a password protected parental controls to be set up.
4. Downloadable apps are available in the app store. Some are free and some have subscriptions.

Resources
https://www.cybercivilrights.org/outreach-and-education/
https://www.cyberrightsproject.com/