

Safe and Secure Online

Parents edition



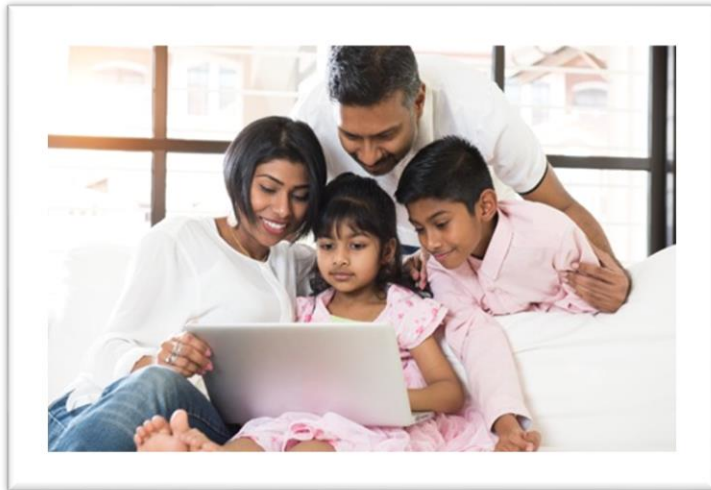
Learn how to surf the web safely and securely for
you and your kids

About Me

- **Name:** Joshua Drew
- **Title:** Information Security Risk Officer
- **Experience:** Over 5+ years of experience in information security. Previously a manager of cybersecurity consulting at a Big 4 Firm (Ernst & Young)
- **Credentials:** CISSP and ISC2 Member
- **Contact Info:** drewj@hvcu.org



UNDERSTANDING THE CYBER WORLD



- Most of us are **Digital Immigrants**.
- Our children are **Digital Natives**.
- They are born into an interconnected world with many hidden dangers.
- Let's start with the most important message...

UNDERSTANDING THE CYBER WORLD

Kids need to
understand:

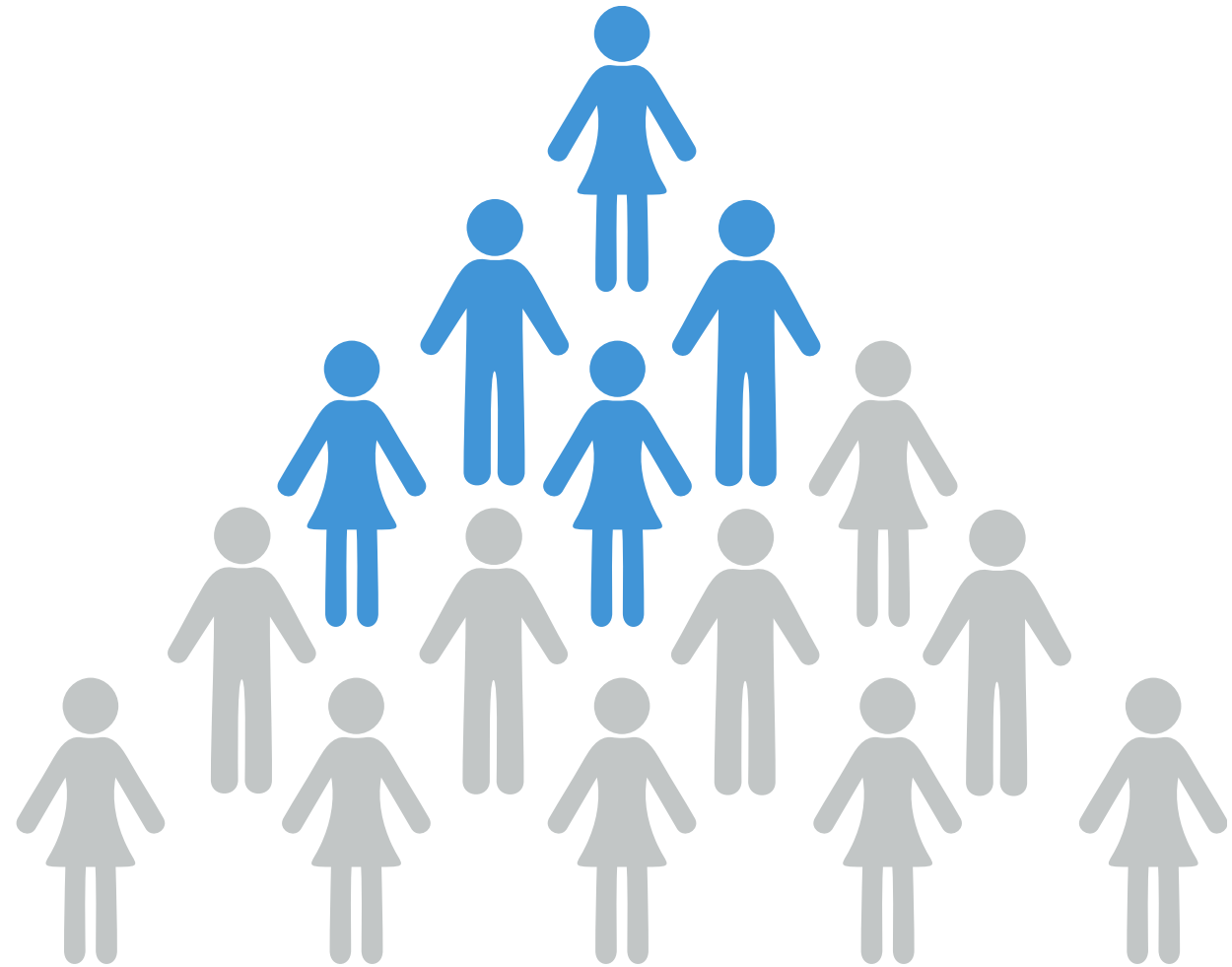
*anything they share
online will stay online
FOREVER.*



UNDERSTANDING THE CYBER WORLD

30%

of children 8-14 use the Internet in a way they know their parents would not approve of.*



Children (n=171)

*Center's Children's Internet Usage Study

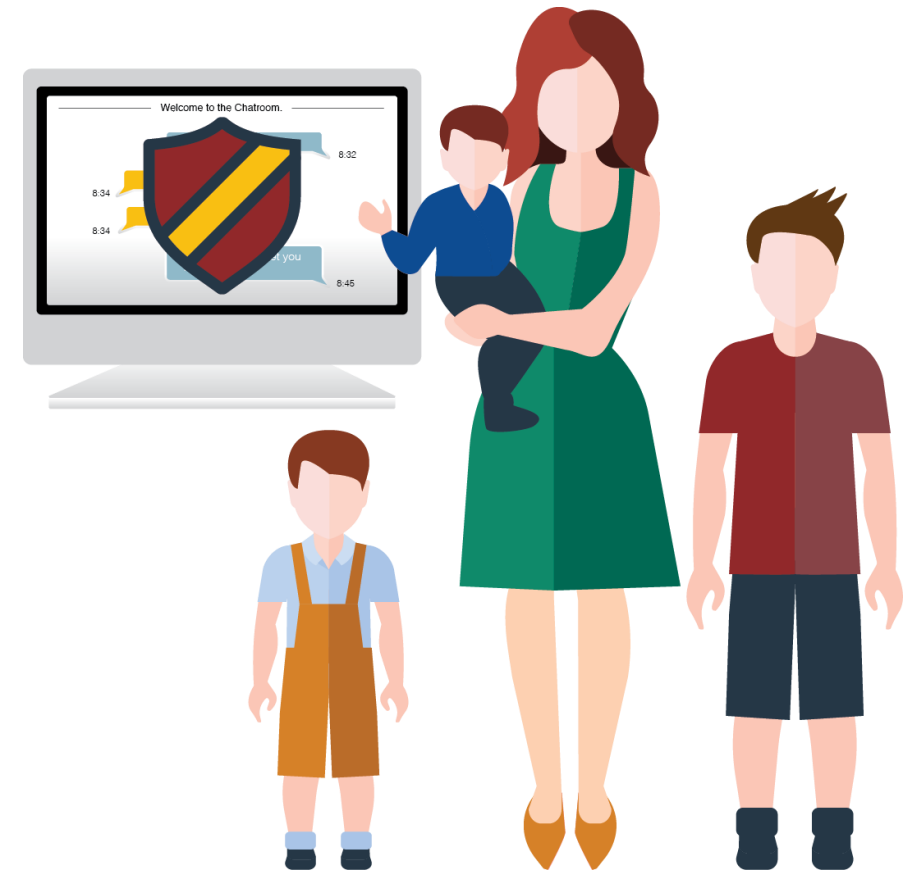
UNDERSTANDING THE CYBER WORLD

- Staying up late chatting and using webcams with strangers
- “Borrowing” parents’ credit cards
- Making poor decisions with personal information
- There are positive ways to use the internet. Start early



THEY CAN SCROLL BEFORE THEY CAN CRAWL.

- Start safety training at a young age.
- Do not wait to begin a dialogue about downloading, cyberbullying, identity theft and more.
- Cyber safety skills should become routine, like looking both ways before crossing the street.
- Don't focus on just the how – also focus on the why



YOU ARE THE CYBER SUPERHERO. IT'S UP TO YOU!

- It's up to parents, guardians and educators
- We should openly share information about what worked and what didn't.



JUST THE FACTS.

ACCORDING TO THE CENTER FOR
CYBER SAFETY AND EDUCATION
CHILDREN'S INTERNET USAGE STUDY:

Over 1/2

of the children surveyed are on the
internet after 10pm on a school
night, not doing homework.



All children answering (n=166)
*Center's Children's Internet Usage Study

JUST THE FACTS.

10%

admit they were late
to school because of
being online late at
night.*



All children answering (n=171)

*Center's Children's Internet Usage Study

JUST THE FACTS.

5%

missed school because they were too tired from being online late.*



WHERE TO BEGIN? ACCESS.

90%

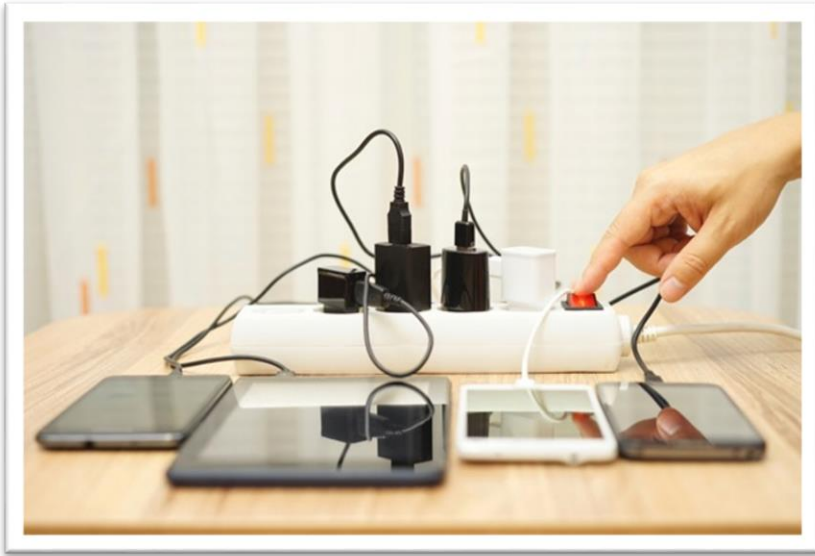
have their phone, tablet or
computer in their room.



All children answering (n=171)

*Center's Children's Internet Usage Study

SET UP SIMPLE ACCESS CONTROLS



- Regulate usage times—*especially at night*.
- Prevent usage in private.
- If there must be a computer in a bedroom, make sure the screen faces the door.
- Keep devices in a central location.
- Set up central charging stations to keep all devices together.

TAKE ADVANTAGE OF BUILT-IN ACCESS CONTROLS

Many devices come with easy
parental controls...

USE THEM.



WHY?

37%

of kids have accidentally visited sites meant for adults.*



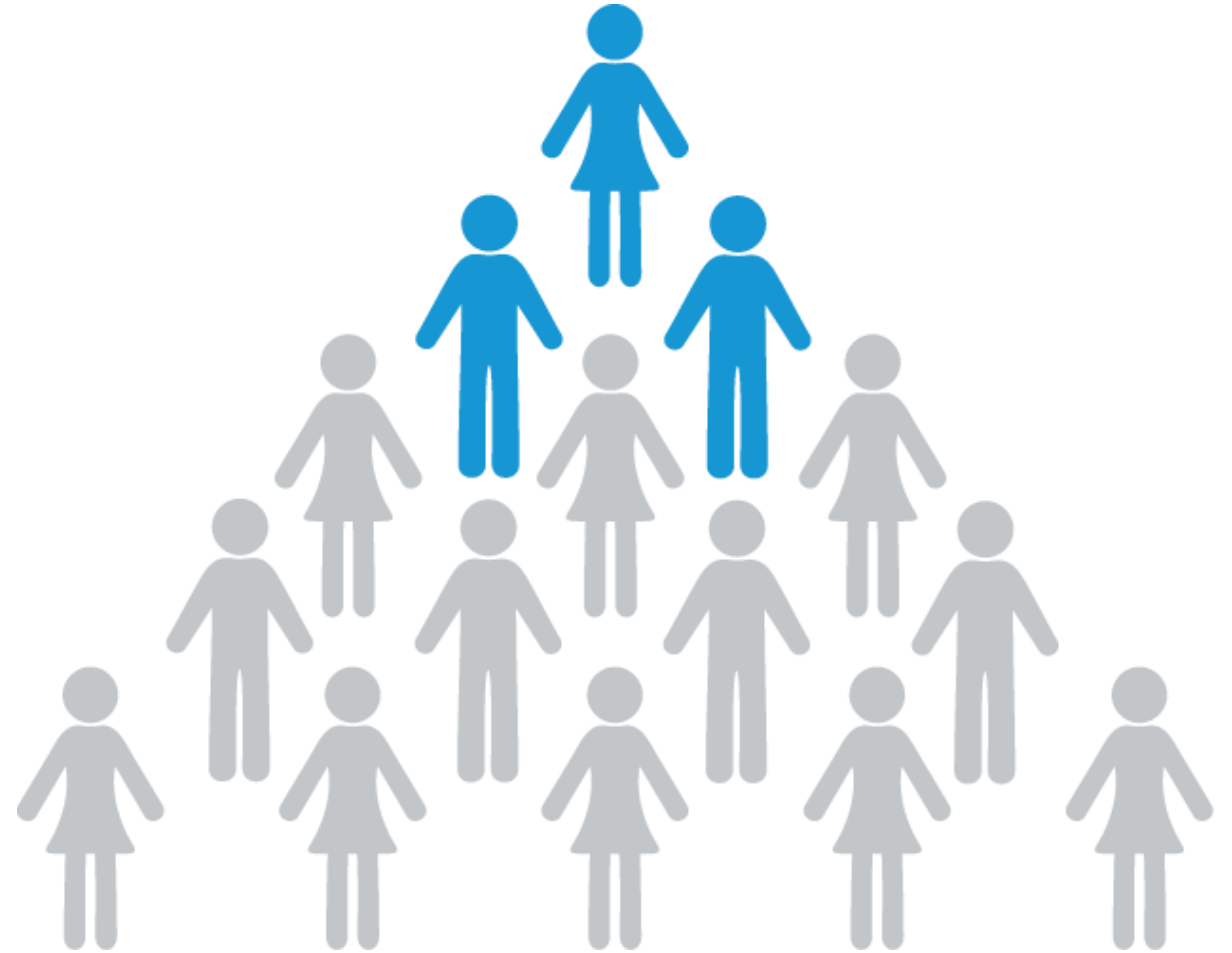
Children (n=171)

*Center's Children's Internet Usage Study

BUT...

20%

are searching for those sites on purpose, and over half follow through with the visit!*



Children (n=171)

*Center's Children's Internet Usage Study

TAKE ADVANTAGE OF BUILT-IN ACCESS CONTROLS

- Many devices can be set up so a child's account cannot be used to download or install apps without parental consent.
- Always set up device controls before giving it to your child.
- Link to parental controls for phones, social media, and more:
<https://www.internetmatters.org/parental-controls/>



15 High Risk Apps
produced by
Sarasota County
Sherriff's Office

FIFTEEN APPS

PARENTS SHOULD KNOW ABOUT

Courtesy of the
Sarasota County Sheriff's Office
UPDATED JULY 2019



MEETME



MEETME is a dating social media app that allows users to connect with people based on geographic proximity. As the app's name suggests, users are encouraged to meet each other in person.

GRINDR



GRINDR is a dating app geared towards gay, bi and transgender people. The app gives users options to chat, share photos and meet up based on a smart phone's GPS location.

SKOUT



SKOUT is a location-based dating app and website. While users under 17 years old are unable to share private photos, kids can easily create an account using a different age.

WHATSAPP



WHATSAPP is a popular messaging app that allows users to send texts, photos, voicemails, make calls and video chats worldwide. WHATSAPP uses an internet connection on smart phones and computers.

TIKTOK



TIKTOK is a new mobile device app popular with kids used for creating and sharing short videos. With very limited privacy controls, users are vulnerable to cyber bullying and explicit content.

BADOO



BADOO is a dating and social networking app where users can chat, share photos and videos and connect based on location. While the app is intended for adults only, teens are known to create profiles.

BUMBLE



BUMBLE is similar to the popular dating app "Tinder" however, it requires women to make the first contact. Kids have been known to use BUMBLE to create fake accounts and falsify their age.

SNAPCHAT




SNAPCHAT is one of the most popular apps in recent years. While the app promises users can take a photo/video and it will disappear, new features including "stories" allows users to view content for up to 24 hours. Snapchat also allows users to see your location.

KIK



KIK allows anyone to contact and direct message your child. Kids can bypass traditional text messaging features. KIK gives users unlimited access to anyone, anywhere, anytime.

LIVEME



LIVE.ME is a live-streaming video app that uses geolocation to share videos so users can find out a broadcaster's exact location. Users can earn "coins" as a way to "pay" minors for photos.

HOLLA



HOLLA is a self-proclaimed "addicting" video chat app that allows users to meet people all over the world in just seconds. Reviewers say they have been confronted with racial slurs, explicit content, and more.

WHISPER



WHISPER is an anonymous social network that promotes sharing secrets with strangers. It also reveals a user's location so people can meet up.

ASK.FM



ASK.FM is known for cyber bullying. The app encourages users to allow anonymous people to ask them questions.

CALCULATOR%



CALCULATOR% is only one of SEVERAL secret apps used to hide photos, videos, files, and browser history.

HOT OR NOT



HOT OR NOT encourages users to rate your profile, check out people in their area, and chat with strangers. The goal of this app is to hook up.

For more information, contact Sarasota County Sheriff's Office Community Affairs at 941.861.4005

SOCIAL MEDIA, NOT SOCIAL MAYHEM



- Can you name these apps? Your kids can.
- Many have age requirements, but it is easy for kids to lie.
- In fact, **30%** of children lie about their age to get onto Facebook—***and many parents and grandparents help them!*** *
- All data provided to a social network is stored, and, most of the time, it is shared by default.

Children (n=171)

*Center 's Children's Internet Usage Study



- Ensure your child's profile is set to Private. Go into settings and adjust the default controls.
- Explain that what is posted on the internet is impossible to remove.
- Make parental approval of social groups or networks part of your child-parent Internet Contract.
- “Friend” or “Follow” your kids so you can check in on their social media activity.

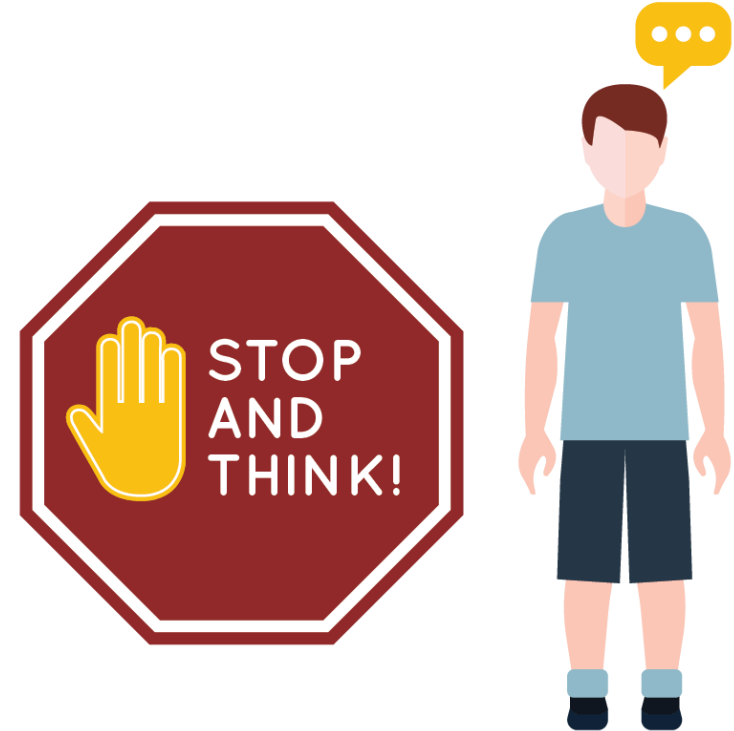
LET YOUR KIDS KNOW:

- Online activity and posts could be available to everyone including future employers and colleges.
- Social media should not become a popularity contest.
- Treat others the way they want to be treated.



LET YOUR KIDS KNOW:

- Stop and think before you post.
- Never share your age, school, address, phone number, last name, vacation information, or when parents are not home.
- Never agree to meet a stranger you met online.
- Use an avatar



A PICTURE CAN BE WORTH MORE THAN YOU KNOW

- Posted photos can reveal too many details.
- Do not post pictures while still on vacation.
- Criminals can use geotagging (and meta data) against you and your kids.



What photos could tell us...

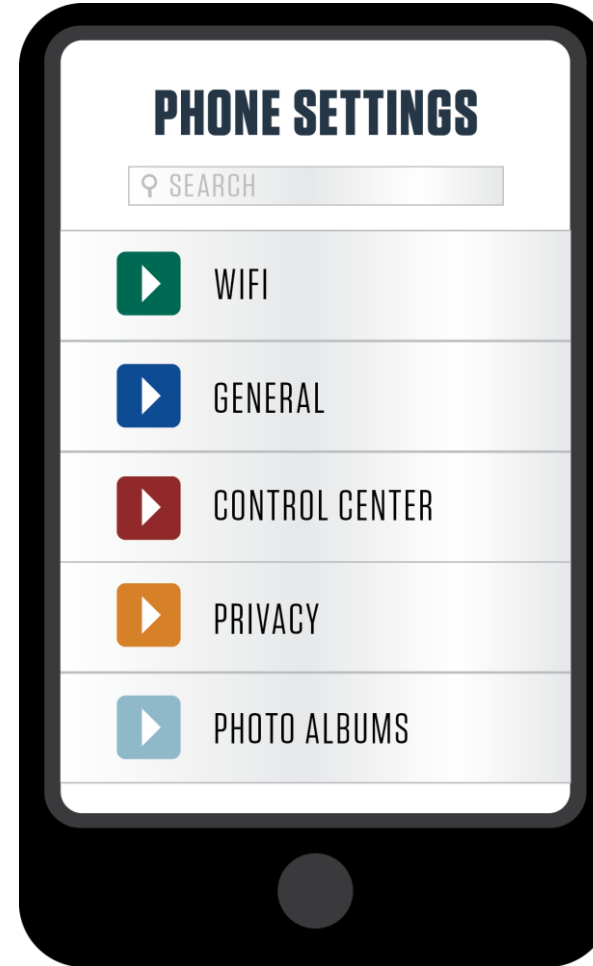


What information are you DRIVING around?



A PICTURE CAN BE WORTH MORE THAN YOU KNOW

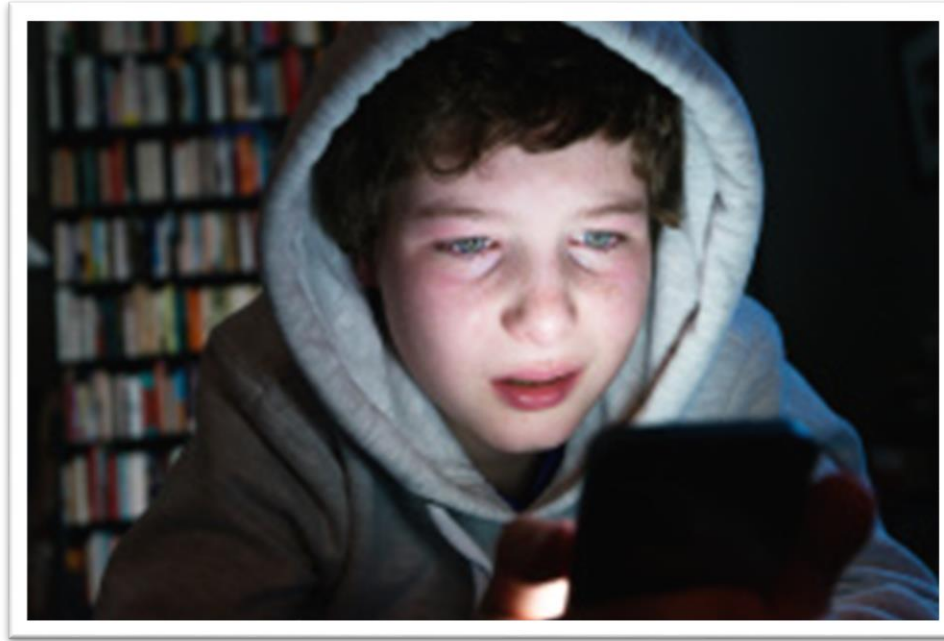
- Only deactivate geolocation from pictures. Leave other geolocation apps and services in place.
- Check with your cellphone provider for instructions on how you can change the settings on your specific device.



CYBERBULLYING

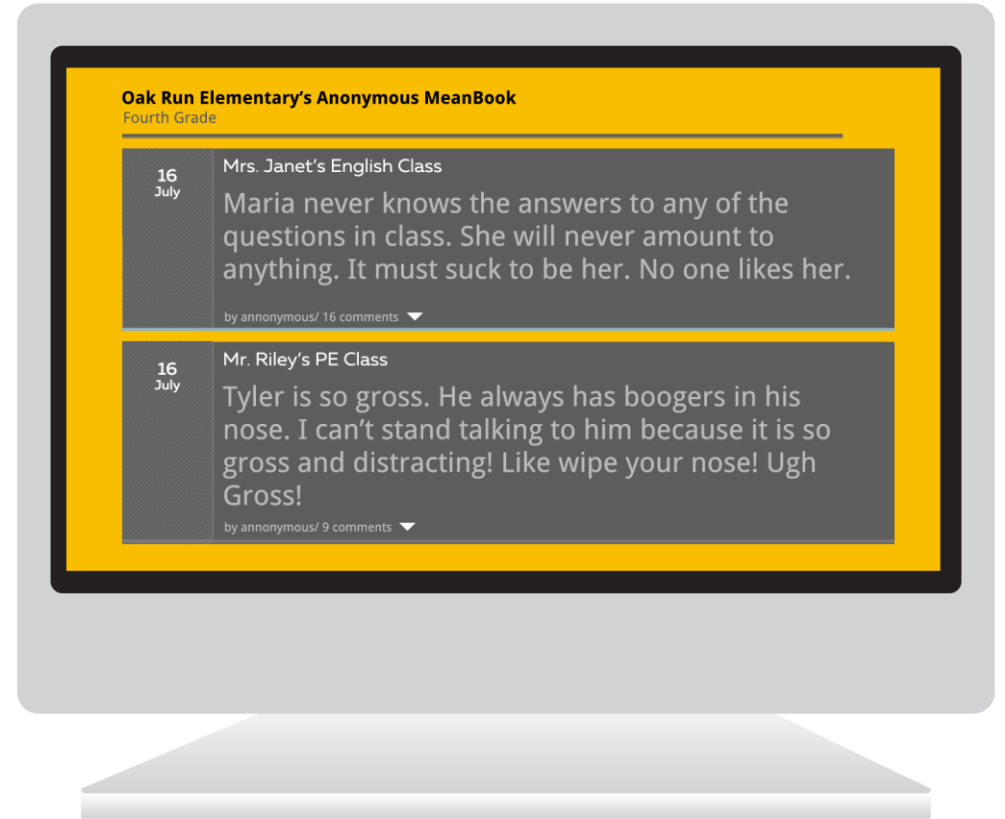
Cyberbullying can happen anywhere hurtful or offensive comments or photos can be sent or posted. (e.g. phones, games, social media)

Compare bullying from years ago to now



CYBERBULLYING

- Children, particularly teens, may not have the same sense of value for their life as adults.
- Teach your kids to confide in you and report any cyberbullying immediately.
- Anonymity is not an excuse to say anything you would not say directly to a person's face.
- Teach them how to report an inappropriate ID online, and block that ID from future interaction.



CYBERBULLYING

- Explain how further steps can be taken to involve police if the person continues inappropriate online activities.
- Save the texts/posts/emails. Don't reply to them and don't delete them.
- Go to the authorities. Children need to know the law protects them.
- Resourceful Link:
<https://www.stopbullying.gov/cyberbullying/how-to-report>



CYBERBULLYING

WATCH FOR THE FOLLOWING SIGNS THAT YOUR CHILD MAY BE THE VICTIM OF CYBERBULLYING:



- Anger, depression, or frustration after using any devices.
- Stops using devices unexpectedly.
- Stops accessing social media sites, apps, or games.
- Uneasy about going to school.
- Abnormally withdrawn from usual friends and family members.

GAMING



THIS IS NOT WHAT TODAY'S
KIDS CONSIDER "GAMING."

THIS IS GAMING

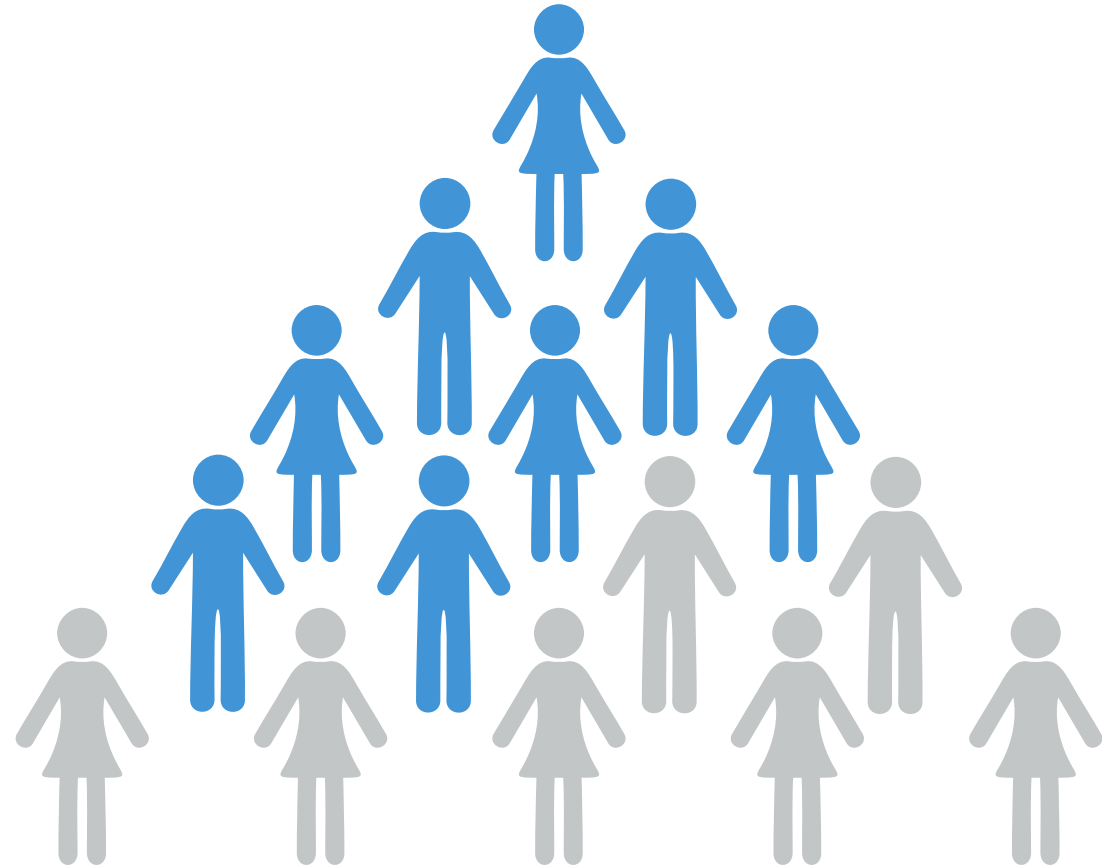
- Games can include violence, murder, and nudity
- And now they are online with strangers using voice chat and at times, video chat



GAMING

50%

of all children are
playing violent games.*



Children (n=170)

*Center's Children's Internet Usage Study

GAMING

- Smartphones and tablets today are powerful
- Restrictions can be implemented in the app store to prevent kids from downloading apps past a certain rating.
- Be vigilant: many app developers build games that allow kids to spend real money for game perks or game currency.
- App restrictions protect not only the child, but they also prevent them from racking up credit card charges.



BBC Sign in Home News Sport Reel Worklife Trav

NEWS

Home Coronavirus Video World US & Canada UK Business Tech Science Stories Entertainment

England Regions Lancashire

Boy, 11, racks up £6,000 online credit card games bill

LIVING EXCLUSIVE

Facebook Twitter Facebook Messenger RSS

This 6-year-old racked up \$16K on mom's credit card playing video games

By Doree Lewak December 12, 2020 | 3:50pm | Updated

BBC Sign in Home News Sport Reel Worklife

NEWS

Home Coronavirus Video World US & Canada UK Business Tech Science Stories Entertai

Tech

'My son spent £3,160 in one game'

By Zoe Kleinman
Technology reporter, BBC News

© 15 July 2019

Delhi teen spends grandad's pension on PUBG store

"The complainant said he received a message on his phone from the bank on May 8," said DCP (North) Anto Alphonse.

Dad Hit with £4,642 Bill After His Kid Splurges on Roblox

140 SHARES Facebook Share Twitter Share Pinterest LinkedIn Print E-mail Reddit

Mike Sanders / 7 months ago

GAMING

- Encourage kids to set up private chats with trusted friends.
- Institute a time limit for game playing (hard/soft lock)
- Know the ESRB rating system. It's similar to movie ratings.



Warning: a popular game with a Teen rating may have a very adult-oriented community of players. These ratings also carry over to smart phones and tablets.

GAMING

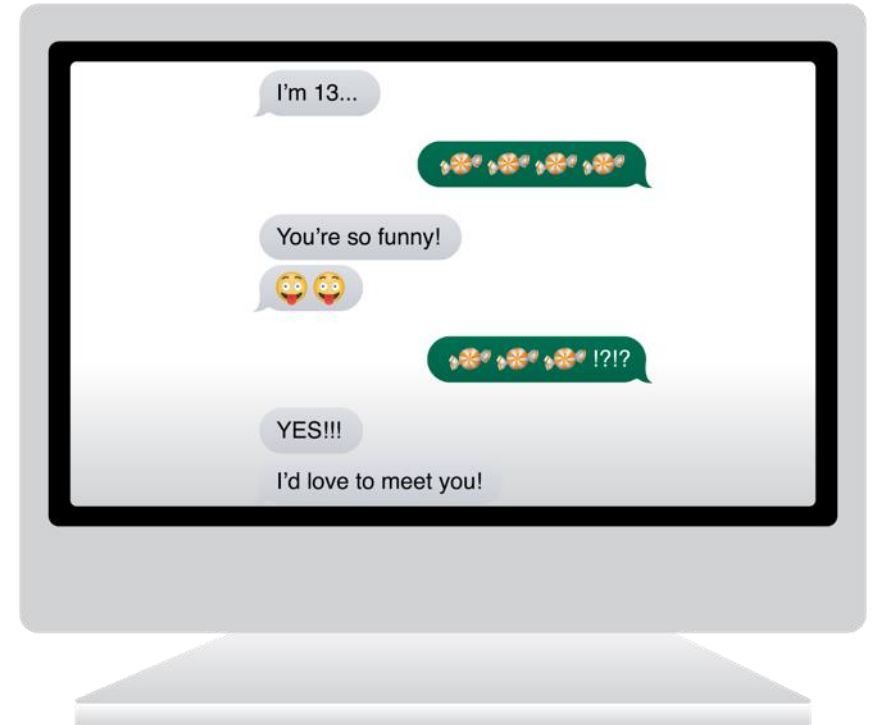
- They can be played online with nearly any device.
- Ability for social networking or micro-transactions for in-game currency.
- Coach your kids to keep online chat conversations relevant to the game.
- Do not provide personal information.
- Many of these social features can be turned off. (set up private chats with friends)



CHATROOMS

Chatrooms can be dangerous; a breeding ground for offensive language and predators.

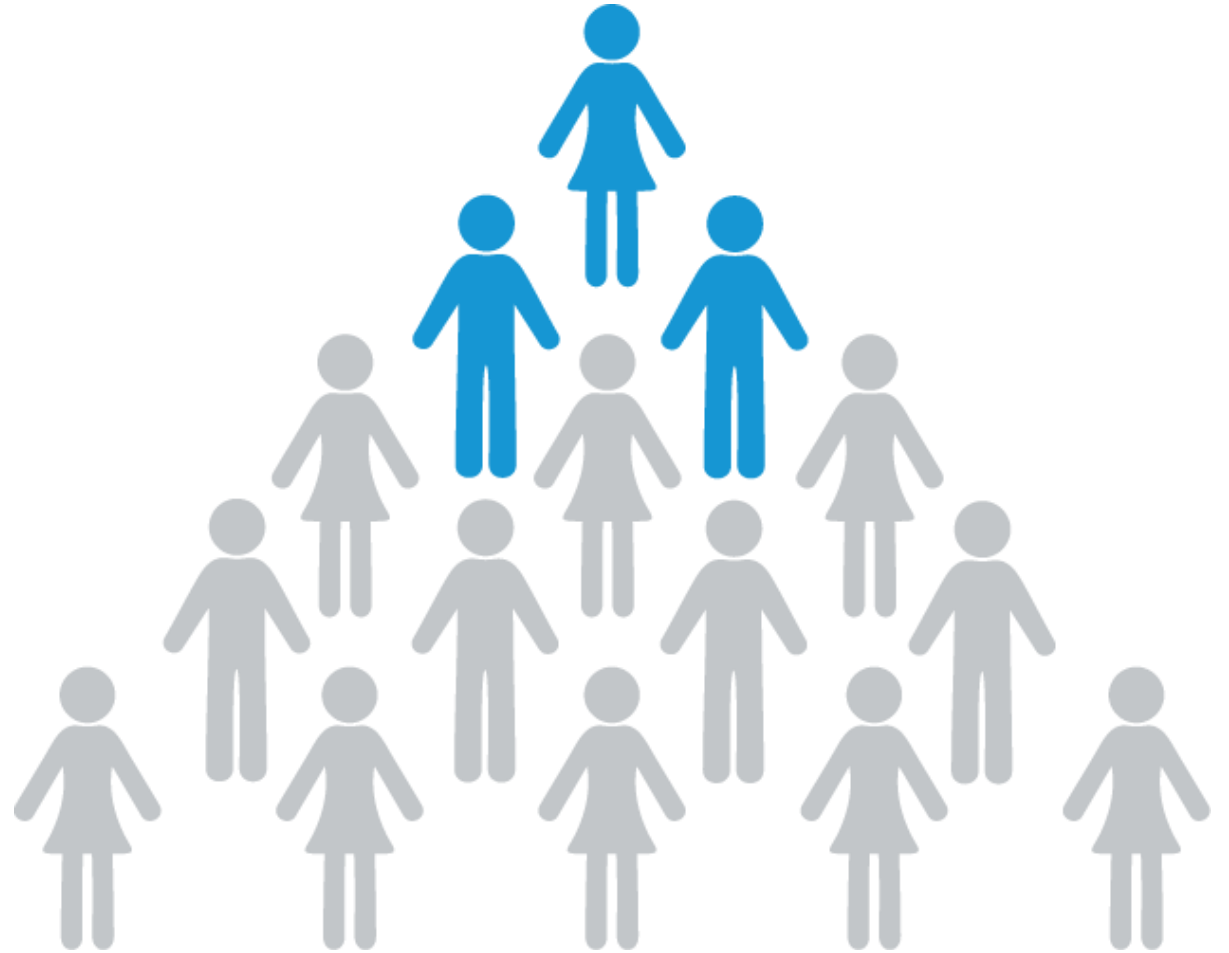
- Many chatrooms also have webcam features.
- Not just on the computer, but in apps
- Children—especially older children—are drawn to the anonymity.
- “Stranger Danger” from the street also applies to chatrooms.



CHATROOMS

21%

of children visited
chatrooms where they
can talk to strangers.*



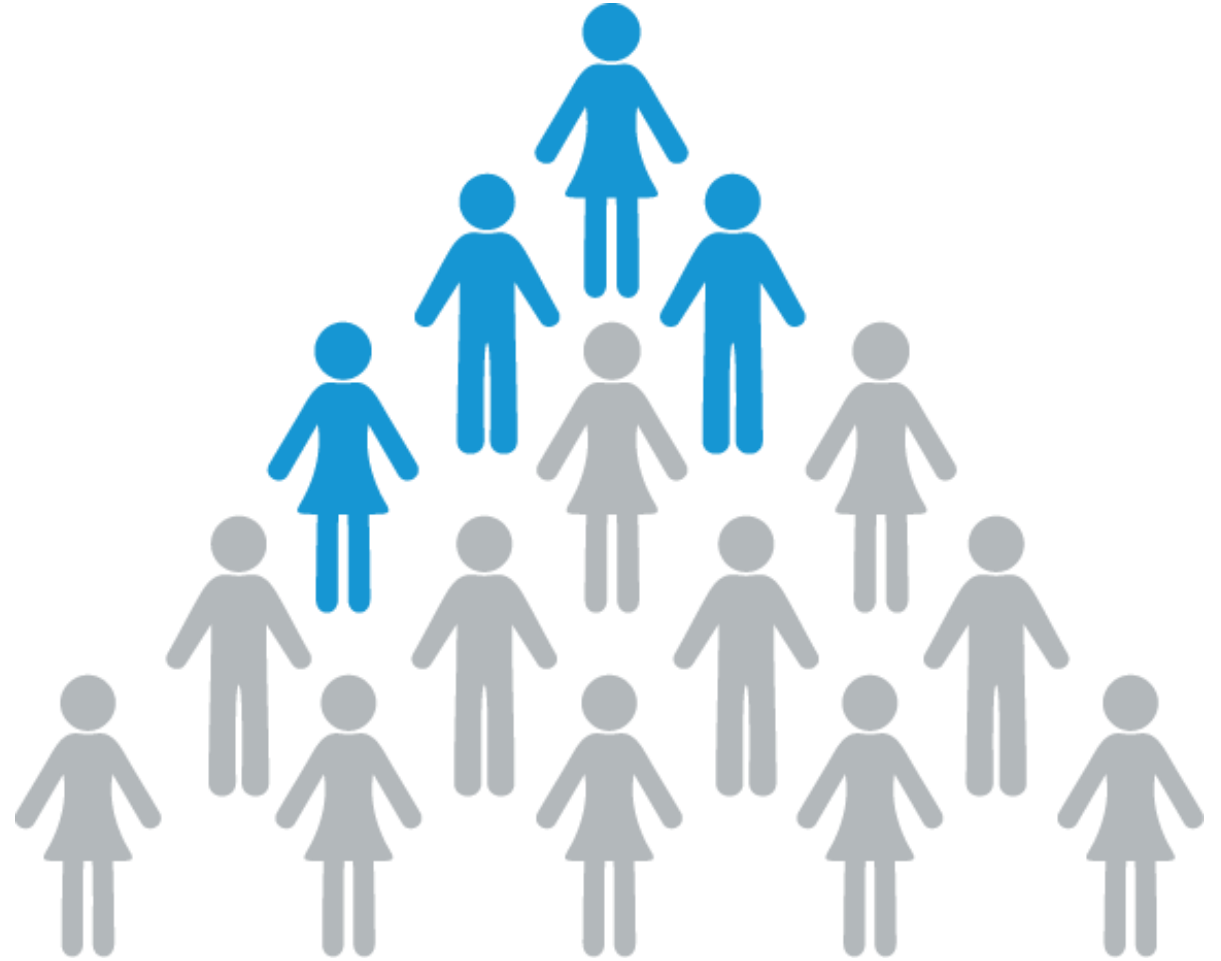
Children (n=170)

*Center's Children's Internet Usage Study

CHATROOMS

25%

of those children gave
a stranger their
phone number.*



All children (n=170).

*Center's Children's Internet Usage Study

CHATROOMS



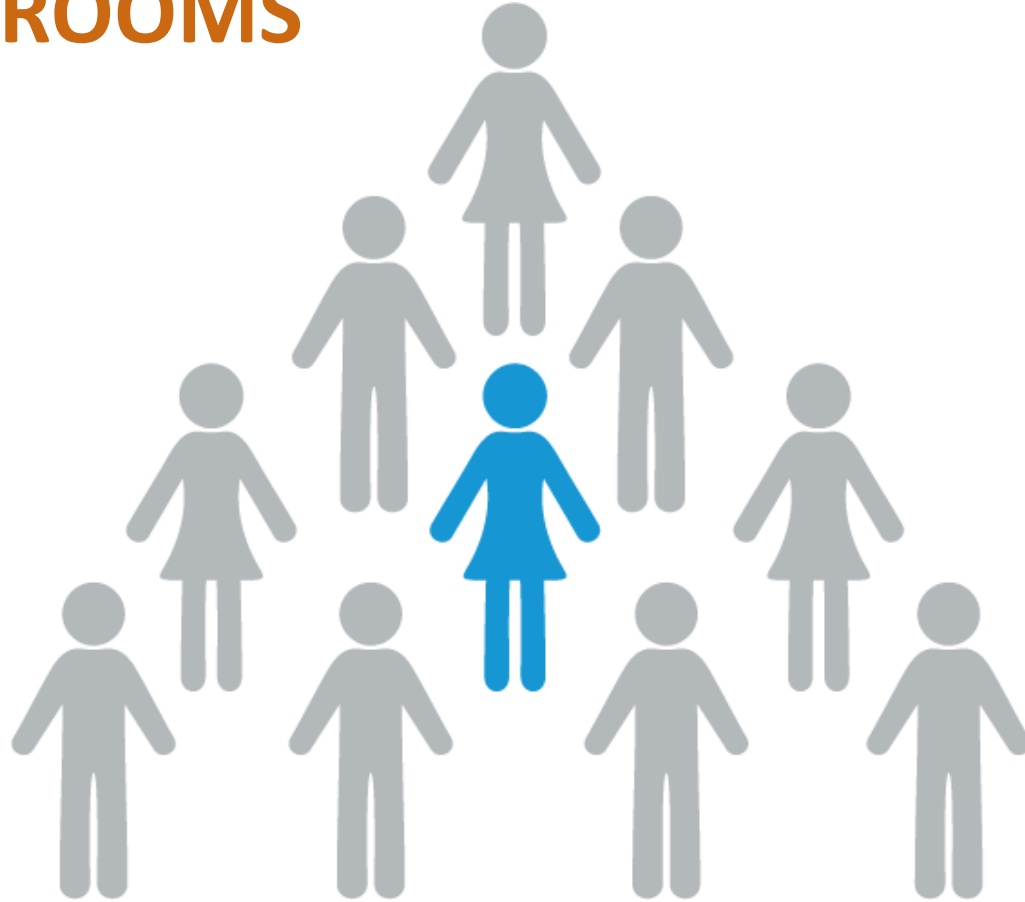
ONE-OUT-OF-FIVE

actually spoke with a stranger.*

All children (n=170).

*Center's Children's Internet Usage Study

CHATROOMS



ONE-OUT-OF-TEN

met a stranger in person.*

All children (n=170).

*Center 's Children's Internet Usage Study

CHATROOMS

IF YOUR CHILDREN VISIT CHATROOMS, THEY SHOULD:

- Remain anonymous.
- Choose an alias that does not give away their name or location.
- Sign out if the topic turns to a sensitive issues.
- Never follow a stranger's instructions, send photos, or download content.

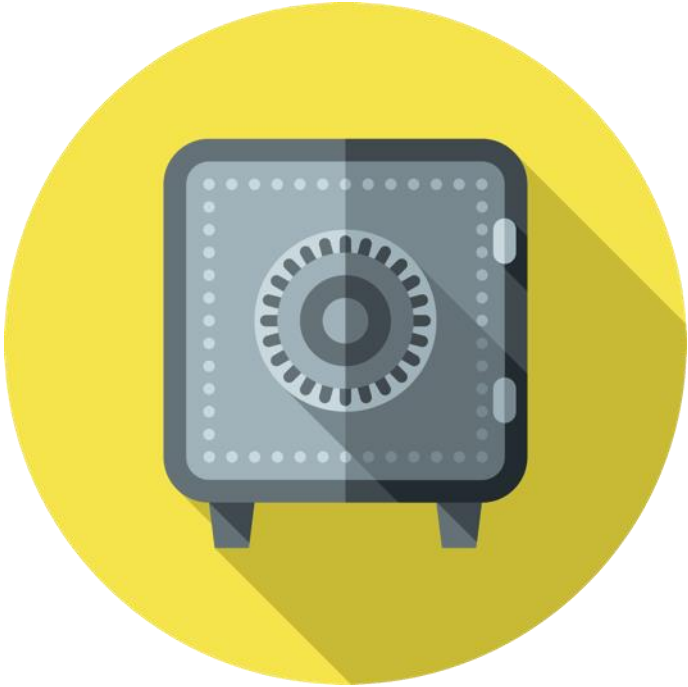


CHATROOMS



YOLO

SAFE PASSWORDS



- Do NOT use the same password on multiple sites
- Make it a phrase- the longer the better!
- 8 character minimum with no repetitive or sequential characters.
- No commonly used passwords and no context-specific words.
- Use a password vault to store all passwords safely.
- Use two factor authentication (2FA) whenever offered.
- Make sure passwords are used on all mobile devices and computers.

Top 10 most common passwords of the year 2020

Position	Password	Number of users	Time to crack it	Times exposed
1. ↑ (2)	123456	2,543,285	Less than a second	23,597,311
2. ↑ (3)	123456789	961,435	Less than a second	7,870,694
3. (new)	picture1	371,612	3 Hours	11,190
4. ↑ (5)	password	360,467	Less than a second	3,759,315
5. ↑ (6)	12345678	322,187	Less than a second	2,944,615
6. ↑ (17)	111111	230,507	Less than a second	3,124,368
7. ↑ (18)	123123	189,327	Less than a second	2,238,694
8. ↓ (1)	12345	188,268	Less than a second	2,389,787
9. ↑ (11)	1234567890	171,724	Less than a second	2,264,884
10. (new)	senha	167,728	10 Seconds	8,213

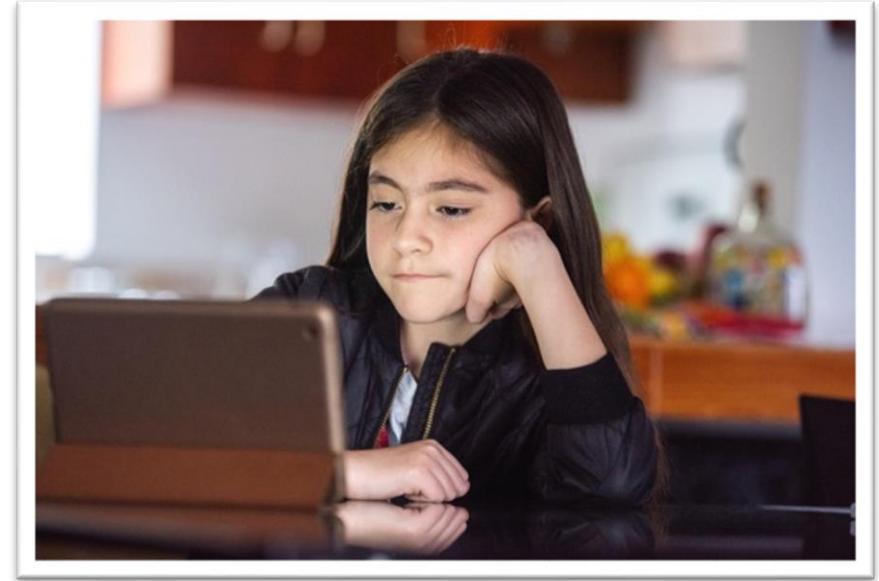
DOWNLOADS



- Speak to your children about the risks of downloading.
- Make sure your antivirus software is updated.
- Only parents should have access to install programs

DOWNLOADS

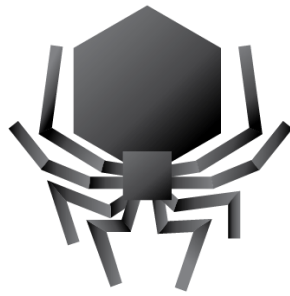
- Downloading games from app stores should be restricted until the child is old enough to make this decision.
- Before handing a phone to your child, make sure they do not have the ability or password to install applications.
- Children should be given information about malware and why it's dangerous to download random things on the Internet.



KNOW YOUR MALICIOUS FROM YOUR SUSPICIOUS.



WORM



VIRUS



TROJAN HORSE



PHISHING

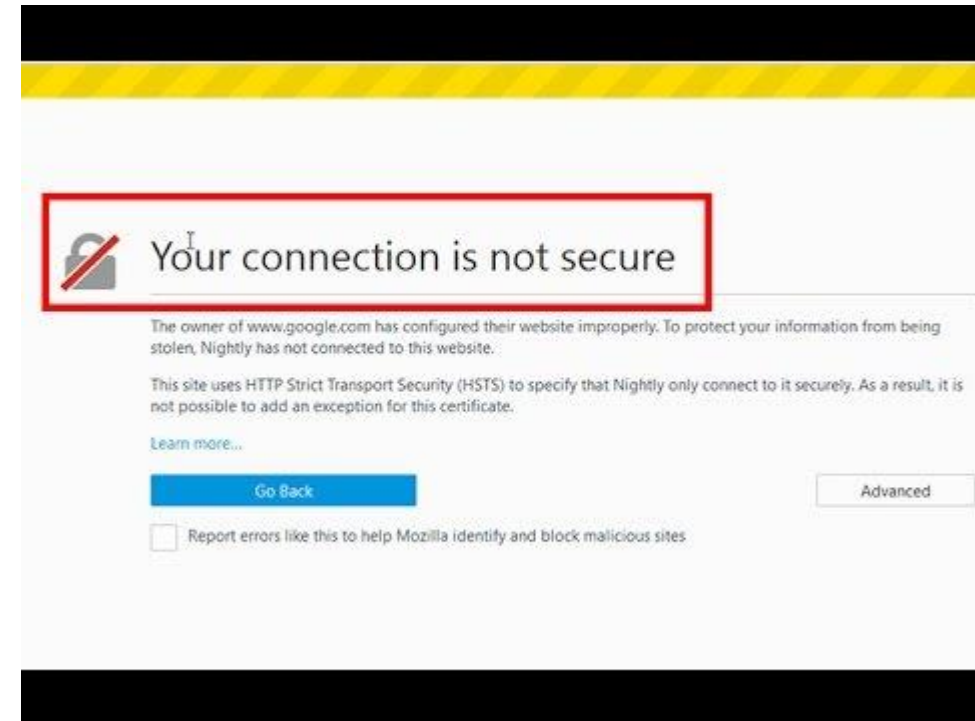
BASIC PRECAUTIONS

- Always start with antivirus software—**but keep it updated!**
- Always update your programs to protect yourself from hackers.
- Involve your children in the process so they understand what is protecting them and why.



BASIC PRECAUTIONS

- Also teach them to pay attention to warnings about a site's safety or expired certificate. These warnings mean—***NO VISITORS ALLOWED!***
- Both your Internet browser and operating system should be updated regularly.



SCAMS. SCUM. THERE'S REALLY NO DIFFERENCE.

- If it's too good to be true, it probably is.
- Phishing emails—emails from someone pretending to be someone else—are a common form of scam.



SCAMS. SCUM. THERE'S REALLY NO DIFFERENCE.

- Do not trust attachments or links from ANY email. Use the “hover” technique!
- Teach your kids how to recognize phishing emails.
- Do not click on or open emails when you do not recognize the sender. Delete them



Look Familiar?

The Apple ID associated with this number is due to be terminated. To prevent this please confirm your details at <http://supportatapple.com/> - Apple Inc.

Text Message
Yesterday 8:26 PM

Hello mate, your FEDEX package with tracking code GB-6412-GH83 is waiting for you to set delivery preferences: e3fmr.info/onAyXsmMMS7

Important Security Alert about your PayPal account. Please click the link bellow to read it: <http://mobile-paypal.com.██████.com>

BACK UP YOUR DATA!

This is extremely important—but, easy to do.

- Simply use an external portable storage device or cloud services.
- Backup your data daily or weekly.



RECAP: TOP TIPS

- Start Early and Keep Talking
- Respect Age Ratings
- Teach Passwords and Privacy
- Use Access Controls
- Protect Identity and Location
- Protect, Update, and Backup
- Know the Signs of Cyberbullying
- Monitor and Communicate

APPENDIX

(resources and links)

Setting up parental controls and privacy settings

- Android:
 - <https://support.google.com/googleplay/answer/1075738?hl=en>
- iOS:
 - <https://support.apple.com/en-us/HT201304>
- Windows 10:
 - <https://news.microsoft.com/en-in/features/windows-10-parental-controls-feature/#:~:text=To%20turn%20on%20parental%20controls,are%20turned%20on%20by%20default.>
- Mac
 - <https://support.apple.com/guide/mac-help/set-up-content-and-privacy-restrictions-mchl8490d51e/mac>
- Router
 - <https://www.cnet.com/how-to/how-to-use-parental-controls-router-pause-wifi-kids-internet/>
- General Search
 - <https://www.internetmatters.org/parental-controls/>
- Xbox
 - <https://www.internetmatters.org/parental-controls/gaming-consoles/xbox-live/>
- PlayStation
 - <https://www.internetmatters.org/parental-controls/gaming-consoles/playstation-network/>
- **Privacy Settings**
 - <https://staysafeonline.org/stay-safe-online/managing-your-privacy/manage-privacy-settings/>

Resources

Parent Resources

<https://www.safeandsecureonline.org/s/>
(Main Content)

<https://staysafeonline.org/>
<https://studentprivacycompass.org/>

<https://www.common sense media.org>
<https://www.connectsafely.org/security/>
<https://www.cisa.gov/publication/stopthinkconnect-parent-and-educator-resources>

Recommended Tools

- **Antivirus**
 - Windows Defender
 - Malwarebytes
 - Bitdefender
- **Monitoring Tools**
 - Netnanny
 - Kasperkey Safe Kids
 - Norton Family
 - Google Family
 - Microsoft Family Safety
- **Password Vaults/Managers**
 - KeePass
 - Bitwarden
 - LastPass
 - Dashlane

Federal laws enabling parents to protect their children's privacy

- **Children's Online Privacy Protection Act (COPPA)** – enacted by congress in 1998, which is regulated by the Federal Trade Commission, not the US Department of Education. The primary goal of COPPA is to allow parents to have control over what information is collected online from their children under age 13.
- **Family Educational Rights and Privacy Act (FERPA)** - a federal law passed in 1974 that bars the disclosure of personally identifiable data in student records to third parties without parental consent.
- **Protection of Pupil Rights Amendment (PPRA)** - was enacted in 1978, and applies to student surveys, instructional materials or evaluations funded by the federal government that deal with highly sensitive issues.
- More info:
https://www.studentprivacymatters.org/ferpa_ppra_coppa/

iDevice restrictions

- Screen Time lets you know how much time you and your kids spend on apps, websites, and more. This way, you can make more informed decisions about how you use your devices, and set limits if you'd like to.

Turn on Screen Time

- Go to Settings > Screen Time.
- Tap Turn On Screen Time.
- Tap Continue.
- Select This is My [device] or This is My Child's [device]





Downtime

Think of this as a nap for your screen time. When you schedule downtime in Settings, only phone calls and apps that you choose to allow are available. Downtime applies to all of your Screen Time-enabled devices, and you get a reminder five minutes before it starts.



Always Allowed

You might want to access certain apps, even if it's downtime or if you set the All Apps & Categories app limit. Phone, Messages, FaceTime, and Maps are always allowed by default, but you can remove them if you want.



App Limits

You can set daily limits for app categories with App Limits. For example, you might want to see productivity apps while you're at work, but not social networking or games. App Limits refresh every day at midnight, and you can delete them any time.



Content & Privacy Restrictions

You decide the type of content that appears on your device. Block inappropriate content, purchases, and downloads, and set your privacy settings with [Content & Privacy Restrictions](#).

Sample Contract

1. It is our phone. We bought it. We pay for it. We are loaning it to you. Aren't we the greatest?
2. We will always know the password.
3. If it rings, answer it. It is a phone. Say hello, use your manners. Do not ever ignore a phone call if the screen reads "Mom" or "Dad". Not ever.
4. You will hand the phone to one of your parents immediately if they ask for it for any reason with no questions asked.
5. Have real life face to face conversations with the people you text. This is a life skill.
6. If it falls into the toilet, smashes on the ground, or vanishes into thin air, you are responsible for the replacement costs or repairs.
7. Do not use this technology to lie, fool, or deceive another human being. Do not involve yourself in conversations that are hurtful to others. Be a good friend first or stay out of the crossfire.
8. Do not text, email, or say anything through this device you would not say in person.
9. Turn it off, silence it, put it away in public—especially in a restaurant, at the movies, or while speaking with another human being. You are not a rude person; do not allow the iPhone to change that.
10. Do not send or receive pictures of your private parts or anyone else's private parts. Don't laugh. Someday you will be tempted to do this despite your high intelligence. It is risky and could ruin your teenage/college/adult life. It is always a bad idea. Cyberspace is vast and more powerful than you. It is near impossible to make anything of this magnitude disappear -- including a bad reputation.

Sample Contract cont.

11. Don't take a zillion pictures and videos. There is no need to document everything. Live your experiences. They will be stored in your memory for eternity.
12. Leave your phone at home sometimes and feel safe and secure in that decision. It is not alive or an extension of you. Learn to live without it. Be bigger and more powerful than FOMO -- fear of missing out.
13. Download music that is new or classic or different than the millions of your peers that listen to the same exact stuff. Your generation has access to music like never before in history. Take advantage of that gift. Expand your horizons.
14. Play a game with words or puzzles or brain teasers every now and then.
15. Keep your eyes up. See the world happening around you. Stare out a window. Listen to the birds. Take a walk. Talk to someone.
16. At lights out we expect your phone to be off. If this does not happen we will take your phone at 8:00PM and return it to you at 7:00 am the next morning.
17. You will receive a brand new iPhone that will easily last 2 years if you take care of it. You are NOT eligible for an upgrade for 2 years unless you pay for it entirely AND both of your parents approve it.
18. You will receive up to \$30 today for a protective case for your new phone. If you want something more expensive or a replacement after today you can ask for it for your birthday or Christmas.
19. You will mess up. We will take away your phone. We will sit down and talk about it. We will start over again. We are always learning. We are on your team. We are in this together.

New Device Safety Tips

1. Change the default password on high-tech toys and gadgets that are Bluetooth- or Wi-Fi-enabled. Most of these items come with a default or generic password that is easy to hack. Change it to something more difficult to guess.
2. Disable photo geotagging on all their devices. Savvy predators can use it to pinpoint your child's location from photos, videos or social media content they post.
3. When buying games as gifts for your kids, make sure you check the age rating and connectivity capabilities and purchase accordingly. Keep in mind that games that allow for interacting with other people online have no restrictions on the age of the other person. Just because a game is rated for younger children doesn't mean an older predator can't play it online, too.
4. Load your child's new device with educational apps and games before you give it to them. There are plenty that offer learning AND entertainment opportunities. Help pick them out
5. Set up a central charging station in your home so kids don't have their devices in their room late into the night. Nine out of 10 children have their phone, tablet or computer in their room (Children's Internet Usage Study, 2016).

New Device Safety Tips Continued

7. Remember to change the password on your Wi-Fi routers and to use built-in settings that establish the level of control your household needs for the kids, such as access times and website category blocking.
8. Before you hand over new devices to your kids, set up non-administrative accounts. This way, they can't change settings or download or install apps without your consent.
9. Remind your kids not to share any personal information, such as their address, phone number or email address. Predators scan for that information and use it to track kids' moves and try to connect with them.
10. Remind your children to report any cyberbullying incidents and to treat others the way they would like to be treated. Be on the lookout for signs that your child is being bullied.
11. Make sure your children know only to connect to trusted Wi-Fi networks and to avoid logging into sensitive accounts like e-mail or social media when they're away from a safe network.

Key Life Moments

Children

Age 3-4
1% own a mobile phone, 16% own a tablet, 0% have a social media profile



Age 5-7
67% of children are online.
Average time spent per week: 8 hours 42 minutes
3% have a social media profile
Children start to browse internet for school work and general browsing

Learn to read & write



4

5

6

7

8

9

10

11

12

13

14

15

16

Age 3-4
55% of parents think the benefits of the internet outweigh the risks
10% think their child knows more about the internet than they do

Age 5-7
35% of parents have never spoken to their children about managing risks online
4% never supervise online access and use

Parents

Under 10
Internet use limited to gaming, streaming video and TV and video calling



Age 8-11
90% of children are online, 49% own a tablet
Average time spent per week: 12 hours and 54 minutes
56% play games online, 12% against people who they've never met

Age 10-11
Phone ownership rises from 21% to 43%



43% of 11 year olds have a social media profile and are messaging, sharing and liking throughout the day

Age 12-13
Phone ownership rises from 50% to 74%
74% of 13 year olds have a social media profile

12-15
98% of children are online
Average time spent per week: 20 hours and 6 minutes
27% play games against people they've never met

Secondary school children use an average of 5 social networks

Start Secondary school



Under 10
Parental concern is limited to sexual content, inappropriate content, violent content and strangers/grooming

Age 10-13
Parental concerns around online bullying increase



Age 5-15
42% of parents have no awareness of content filters

Age 5-15
16% of parents have never spoken to their child about managing risks online



Age 12-15
8% of parents do nothing to regulate or monitor their child's activity online



Source: 2016 OFCOM Children and parents: media use and attitudes report, 2013 Cybersafe Report

(ISC)[®]

Safe and Secure Online[®]
by the Center for Cyber Safety and Education

www.IAmCyberSafe.org



@IAmCyberSafe



@IAmCyberSafe



@Center for Cyber Safety and Education



@ISC2Cares

© 2016 Center for Cyber Safety and Education, a 501(c)(3) segregated fund of (ISC)², Inc. Permission granted to reproduce for personal and educational use only. Commercial copying, hiring, lending is prohibited.