(ISC)²®

Safe and Secure Online®

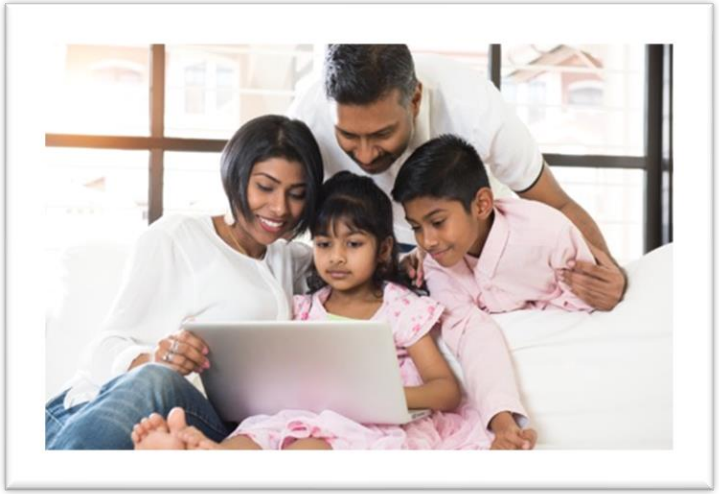
by the Center for Cyber Safety and Education

PARENTS EDITION

CENTER FOR
**CYBER SAFETY
AND EDUCATION**

This presentation has been created by the Center for Cyber Safety and Education with the help of the world's leading cybersecurity professionals: the certified global members of (ISC)^2.

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.

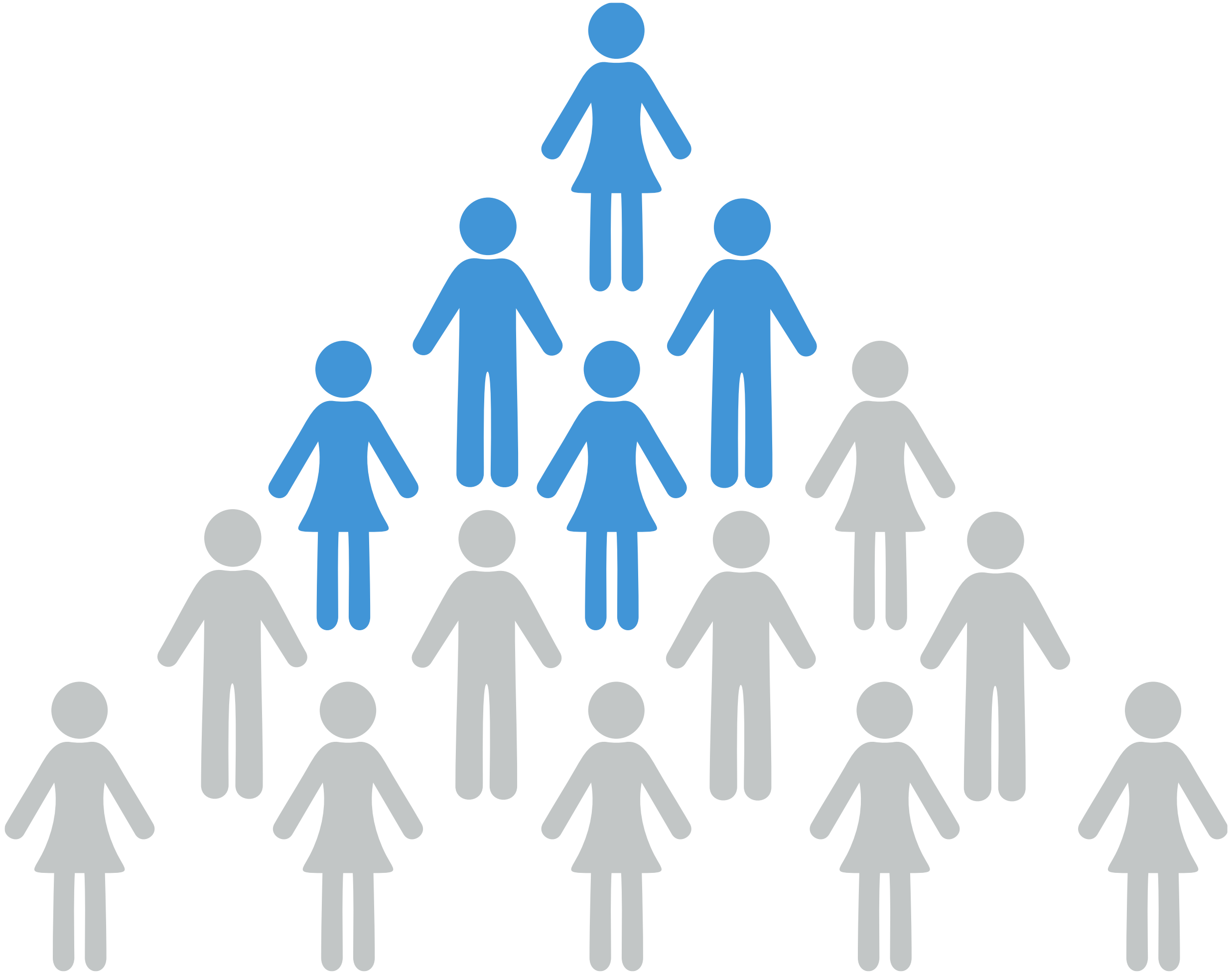
UNDERSTANDING THE CYBER WORLD

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.*



Children (n=171)

*Center's Children's Internet Usage Study

UNDERSTANDING THE CYBER WORLD

- Chatting and using webcams with strangers
- “Borrowing” parents’ credit cards
- Making poor decisions with personal information

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.

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.

All children answering (n=171)
*Center's Children's Internet Usage Study

WHERE TO BEGIN?
ACCESS.

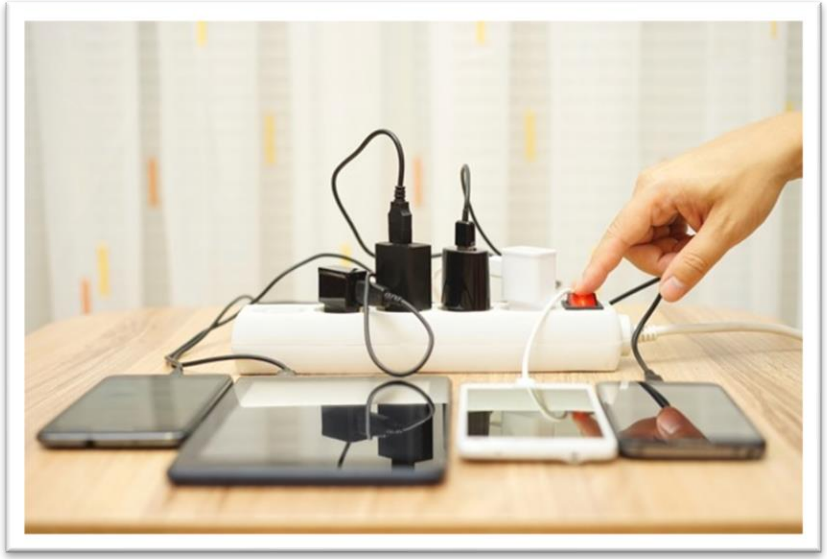
90%

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

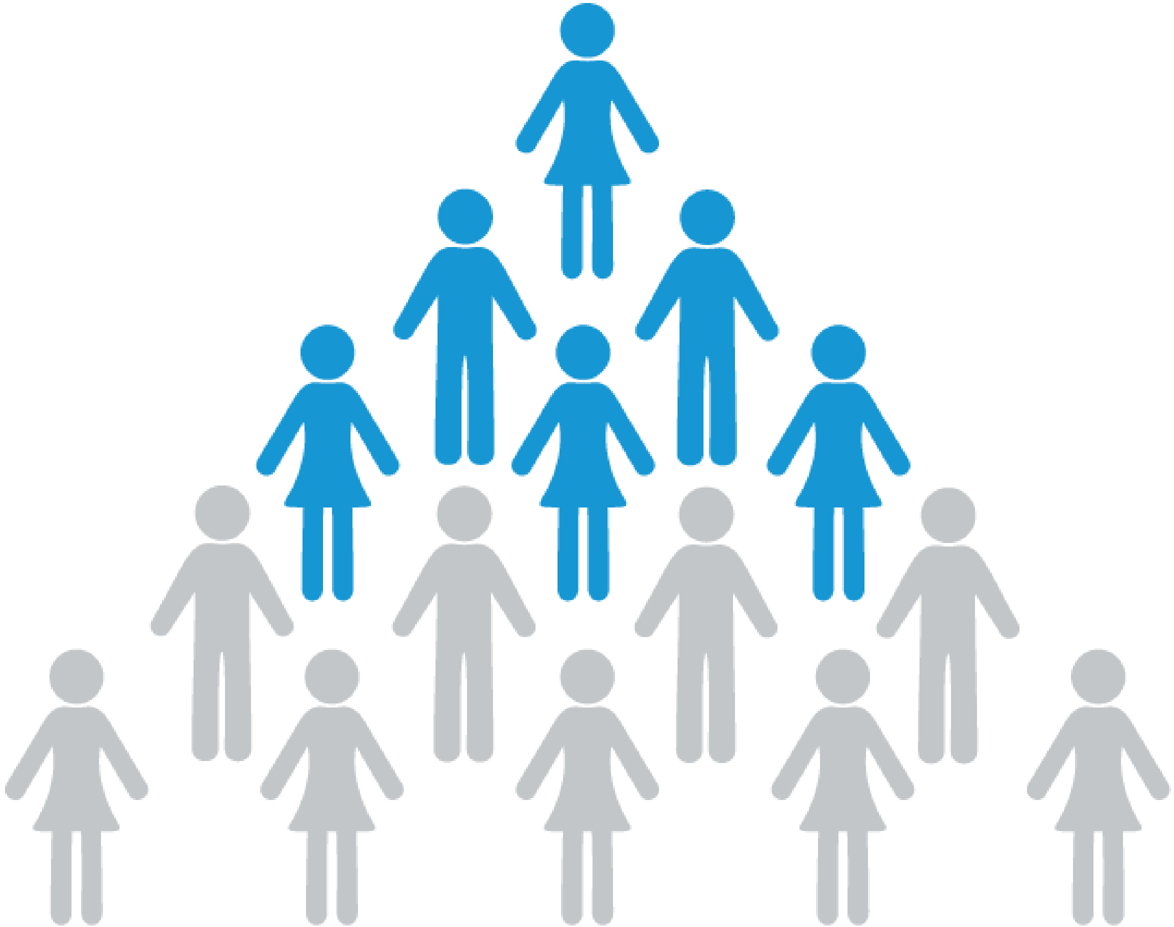
Many devices come with easy parental controls…

USE THEM.

WHY?

37%

of kids have accidentally visited sites meant for adults.*



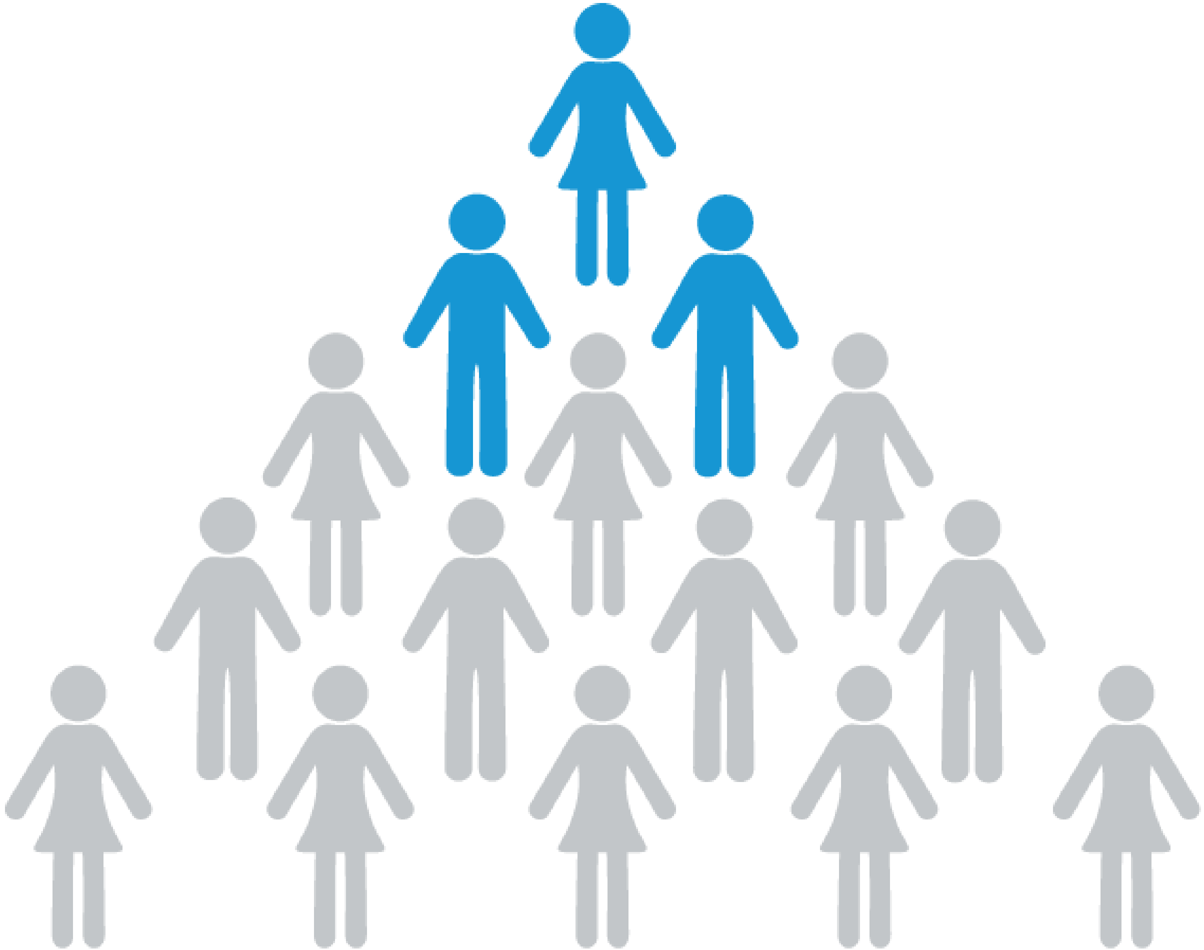
Children (n=171)

*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)

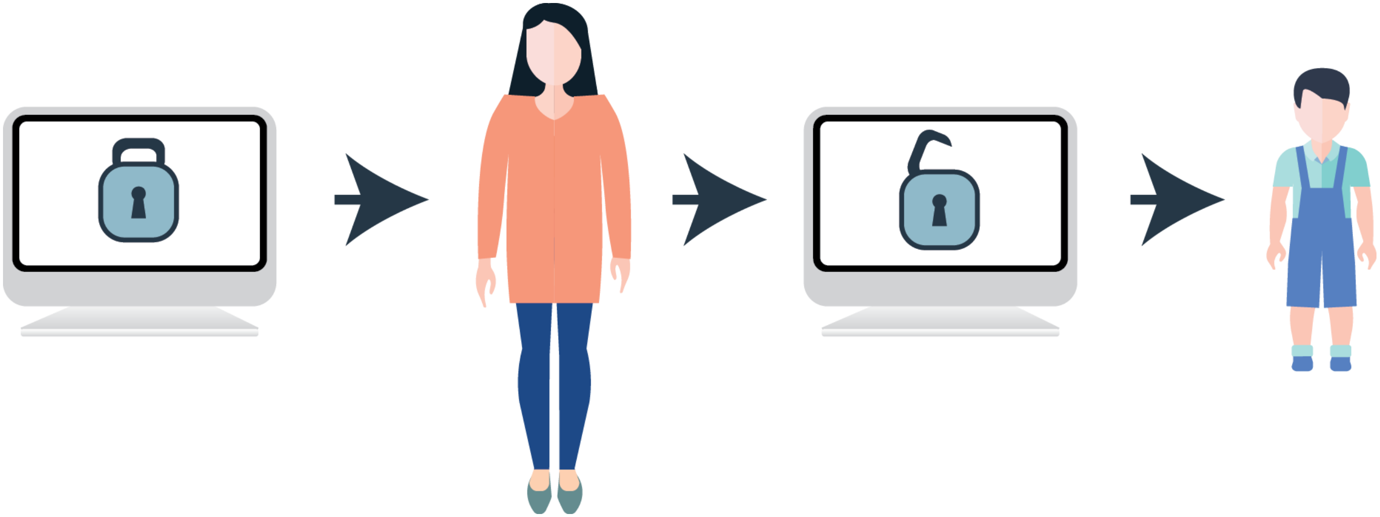
*Center's Children's Internet Usage Study

TAKE ADVANTAGE OF BUILT-IN ACCESS CONTROLS

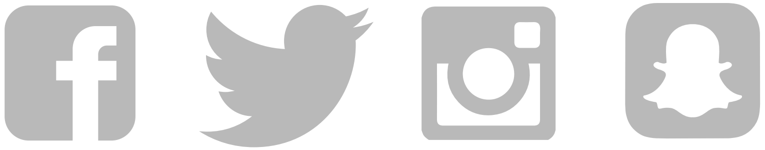
- Many devices can be set up so a child’s account cannot be used to download or install apps without parental consent.
- Always set up device controls before giving it to your child.

FOR EVEN GREATER CONTROL:

Create all of your child's online passwords for them and require the child to have you input them before use of online accounts or purchasing apps.



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.

INSTASNAP
search
MARIA ESPINOZA
7th grade: Forest Middle
FRIENDS
March 20, 2016
Lazy day on the beach for spring break.
March 18, 2016
Traveling to Laguna Beach, California

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.

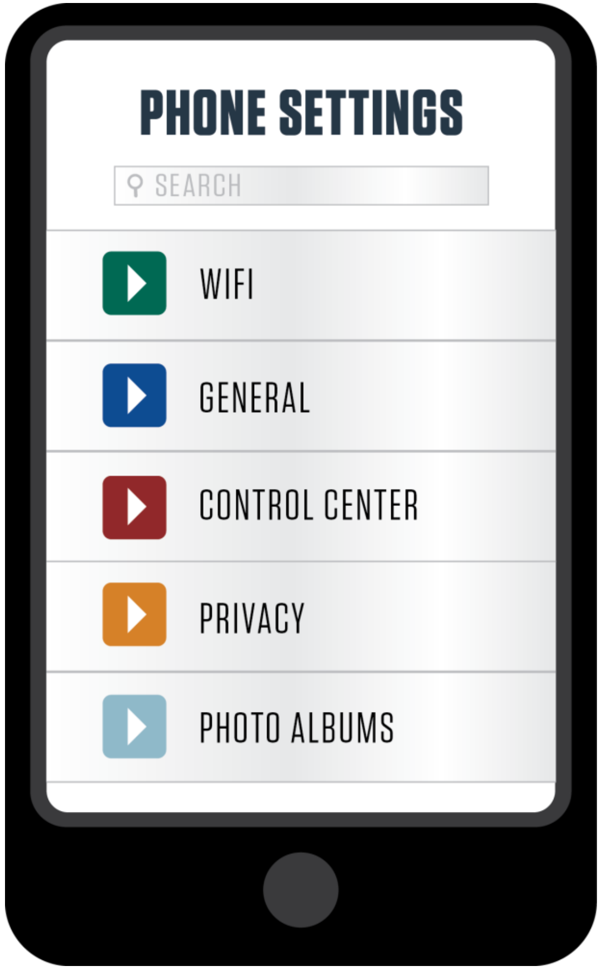
A PICTURE CAN BE WORTH MORE THAN YOU KNOW

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

A PICTURE CAN BE WORTH MORE THAN YOU KNOW

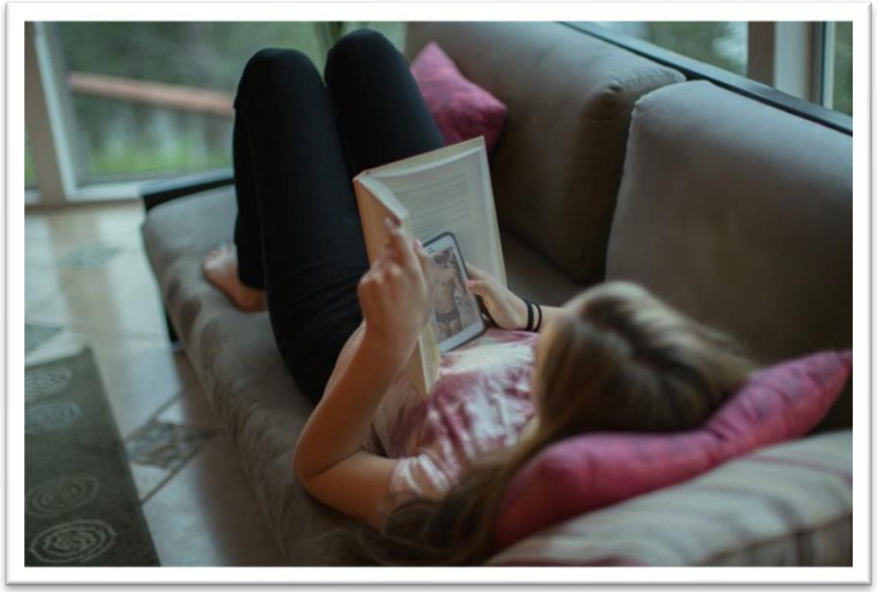
- Only deactivate geolocation from pictures. Leave other geolocation apps and services in place.

- Check with your cellphone provider for instructions on how you can change the settings on your specific device.



SEXTING

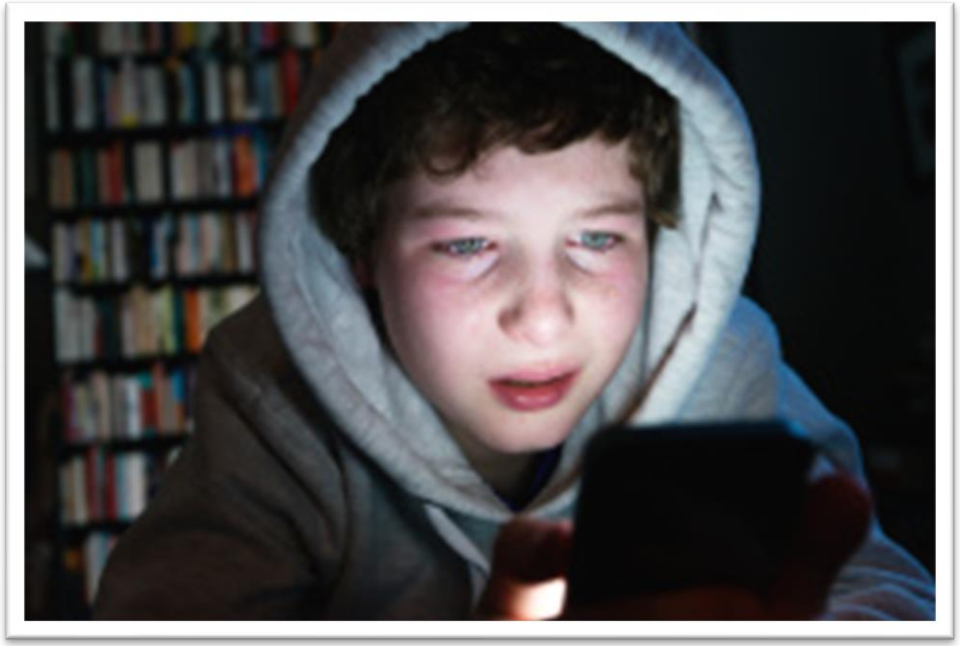
Talk to your kids about taking and sharing sexually explicit photos.



- Using a picture messaging app does not mean the photo will really disappear within seconds.
- Take a screen shot with your phone of a picture message so your child can see: ***nothing is truly secret or deleted once it is sent.***

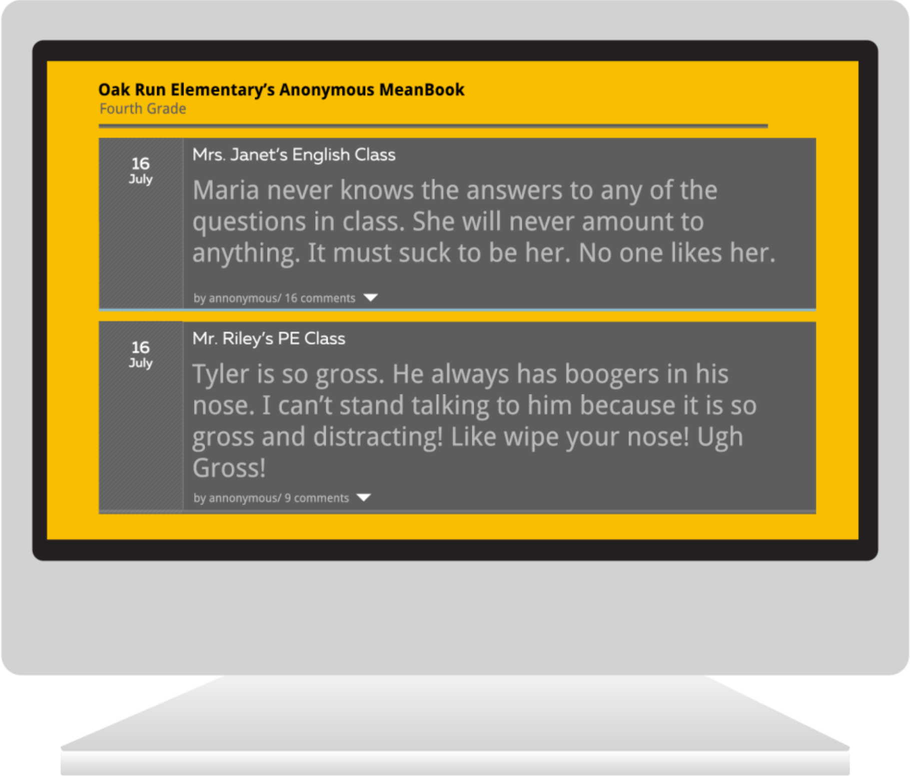
CYBERBULLYING

Cyberbullying can happen anywhere hurtful or offensive comments or photos can be sent or posted.



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.



Oak Run Elementary's Anonymous MeanBook
Fourth Grade

16 July

Mrs. Janet's English Class

Maria never knows the answers to any of the questions in class. She will never amount to anything. It must suck to be her. No one likes her.

by annonymous/ 16 comments ▼

16 July

Mr. Riley's PE Class

Tyler is so gross. He always has boogers in his nose. I can't stand talking to him because it is so gross and distracting! Like wipe your nose! Ugh Gross!

by annonymous/ 9 comments ▼

CYBERBULLYING

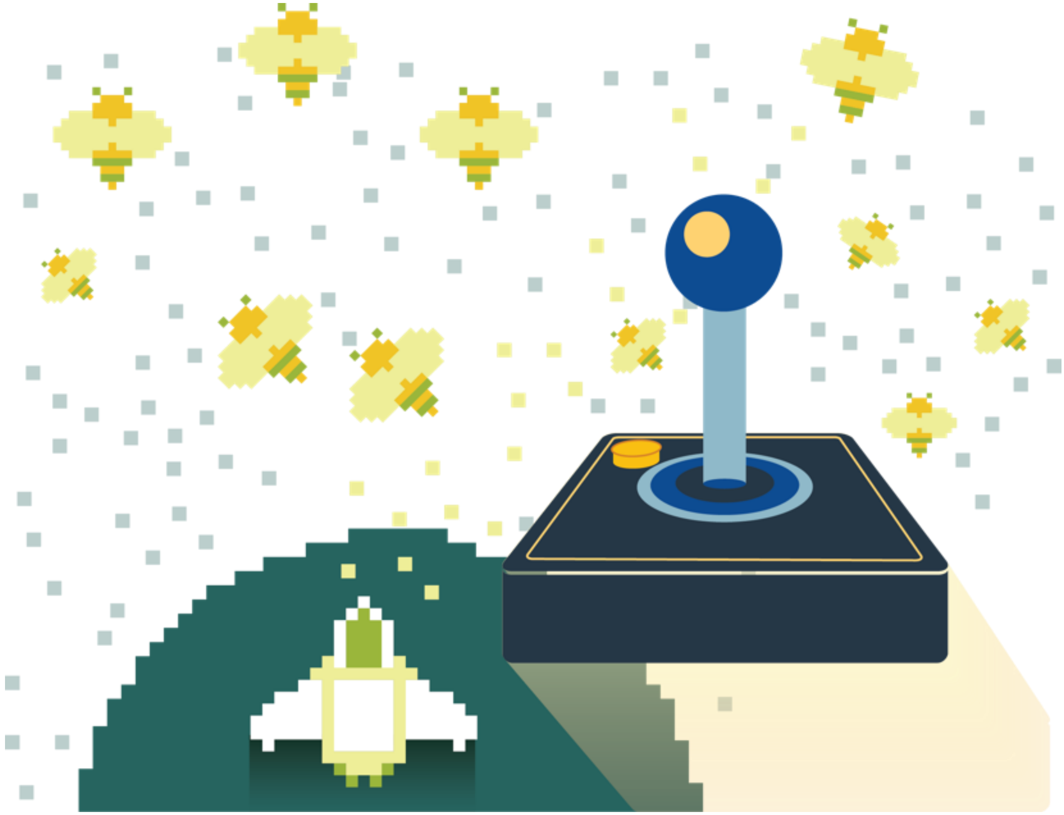
- Explain how further steps can be taken to involve police if the person continues inappropriate online activities.
- Save the texts/posts/emails. Don't reply to them and don't delete them.
- Go to the authorities. Children need to know the law protects them.

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.”

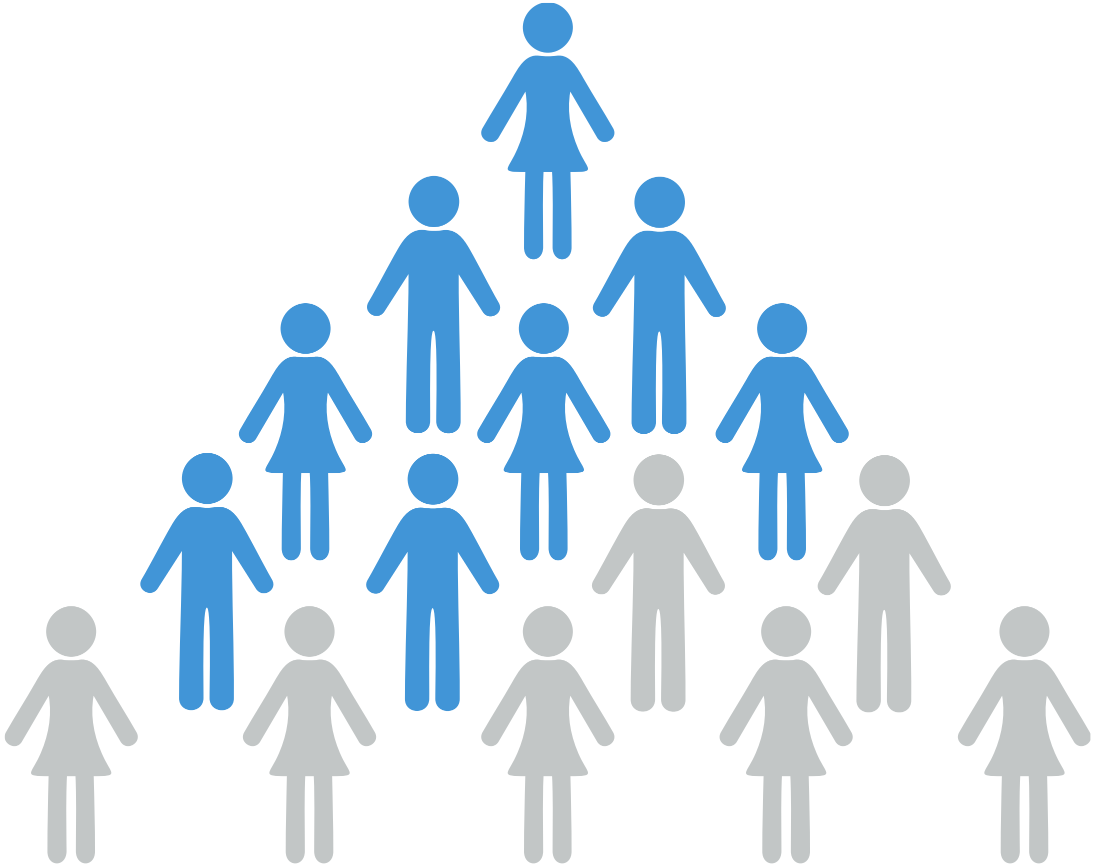
THIS IS GAMING

- Games can include violence, murder, nudity, and prostitution.
- And now they are online with strangers.

GAMING

50%

of all children are playing violent games.*



Children (n=170)

*Center's Children's Internet Usage Study

GAMING

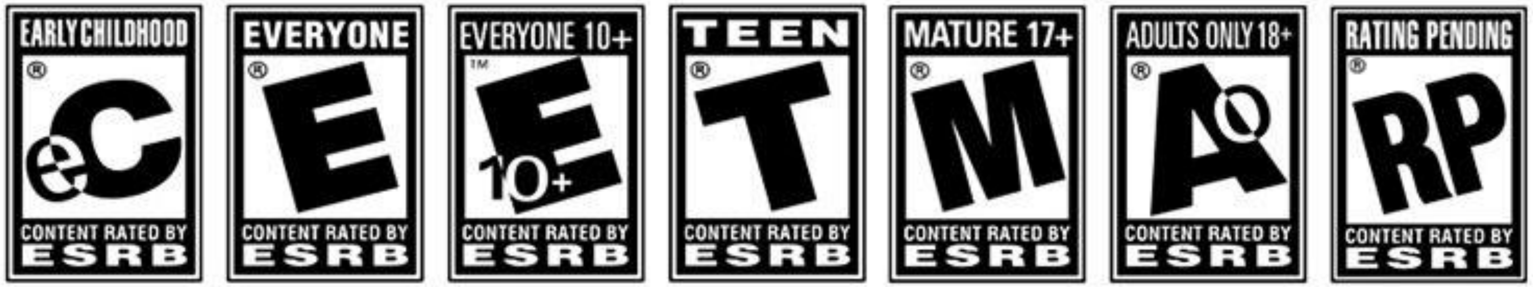
- Restrictions can be implemented in the app store to prevent kids from downloading apps past a certain rating.

- 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.

GAMING

- Encourage kids to set up private chats with trusted friends.
- Institute a time limit for game playing.
- 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.

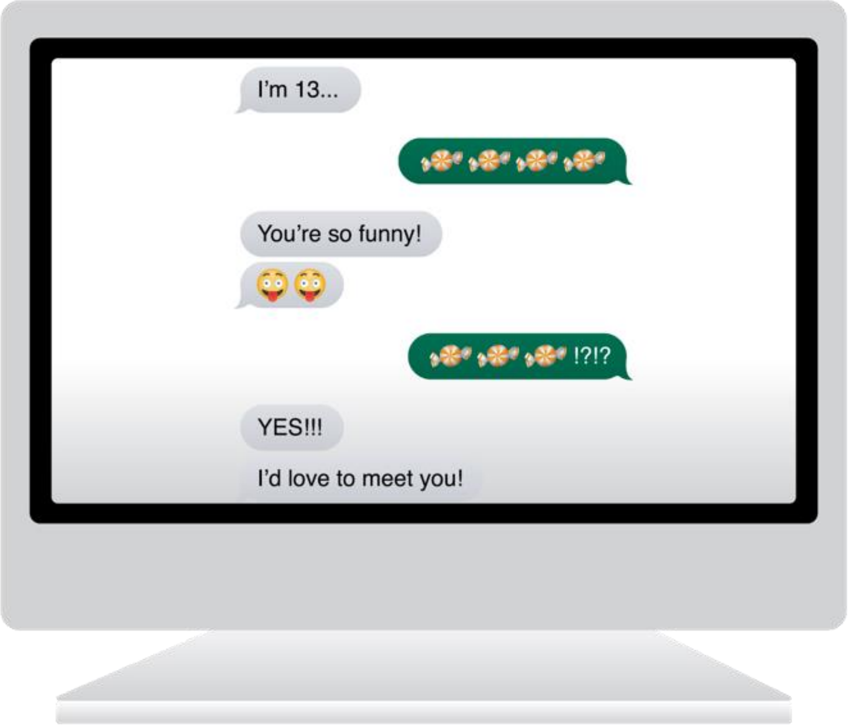
GAMING

- 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.

CHATROOMS

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

- Many chatrooms also have webcam features.
- Children—especially older children—are drawn to the anonymity.
- “Stranger Danger” also applies to chatrooms.



I’m 13...

🍬🍬🍬🍬

You’re so funny!

😛😛

🍬🍬🍬 !?!?

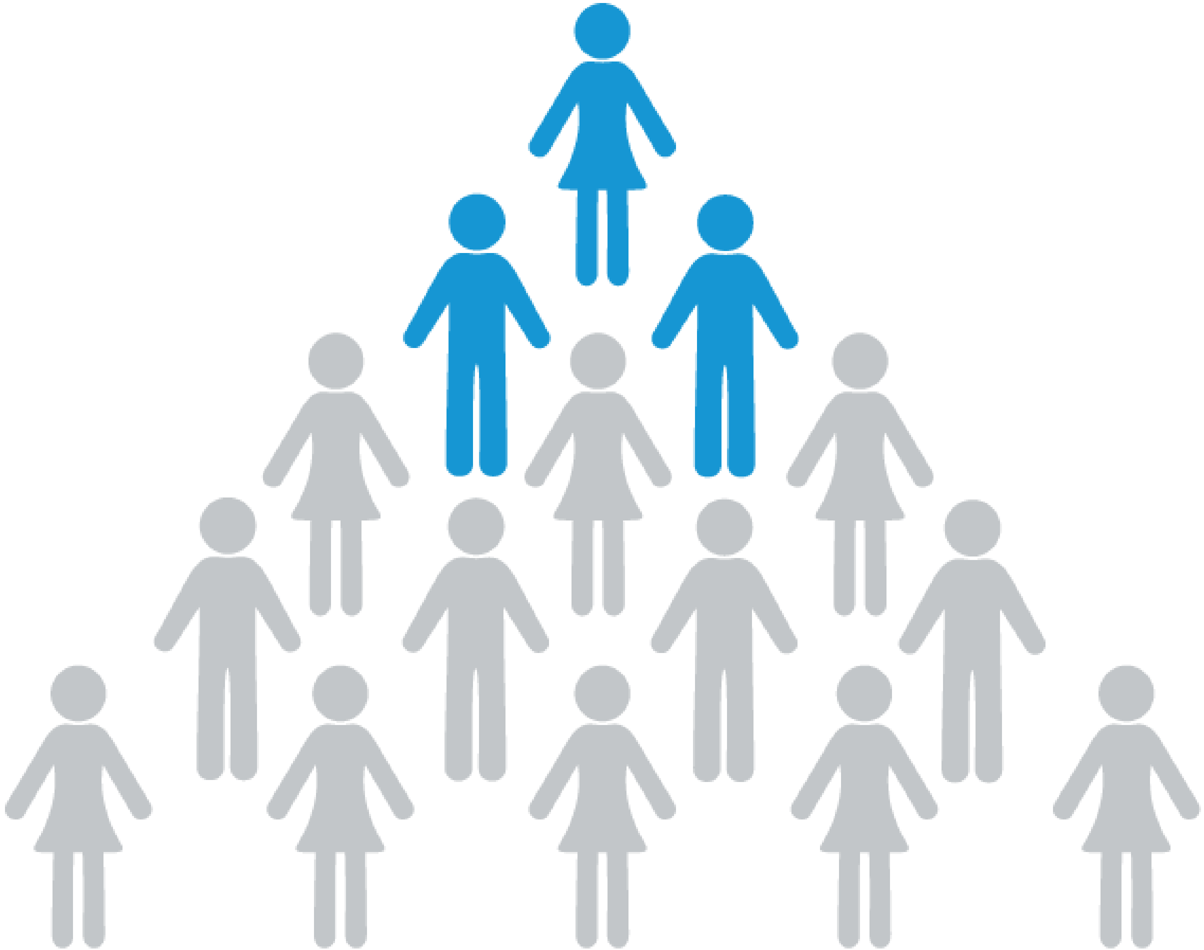
YES!!!

I’d love to meet you!

CHATROOMS

21%

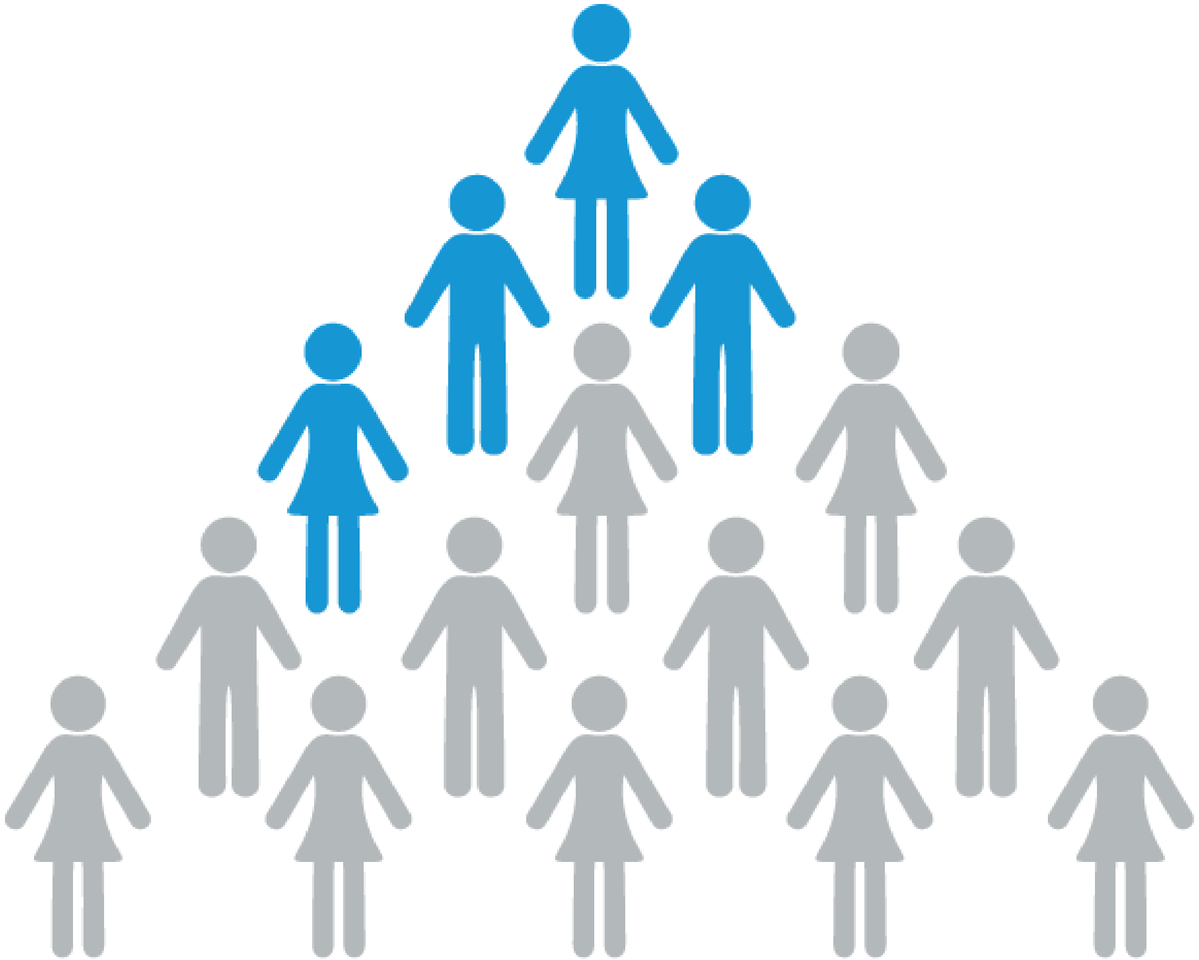
of children visited chatrooms where they can talk to strangers.*



Children (n=170)

*Center's Children's Internet Usage Study

CHATROOMS



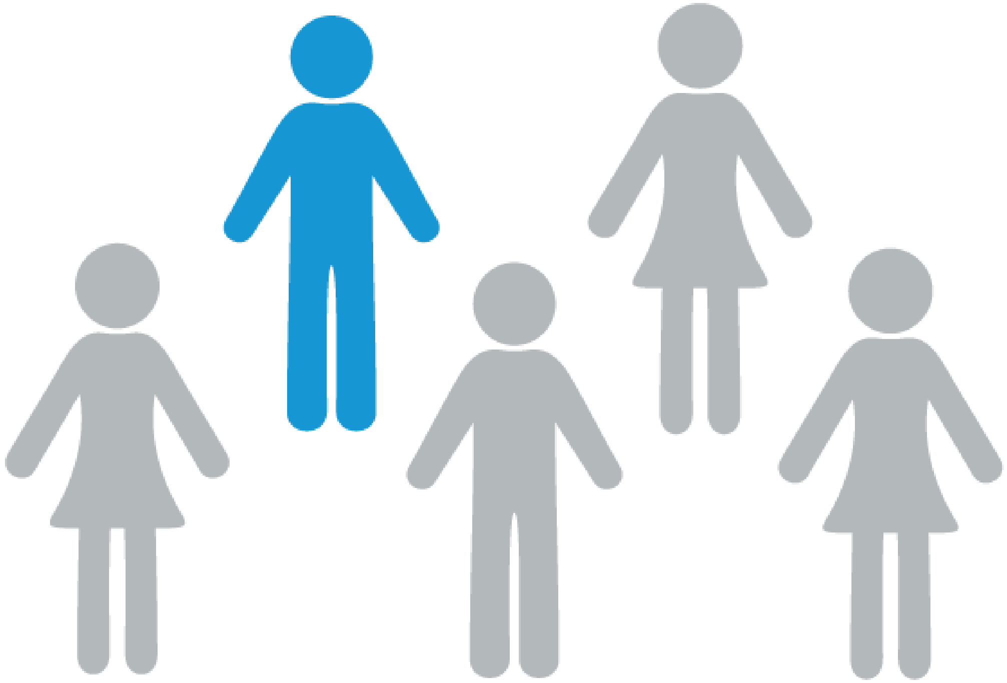
25%

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 issue like sex and drugs.
- Never follow a stranger's instructions, send photos or download content.

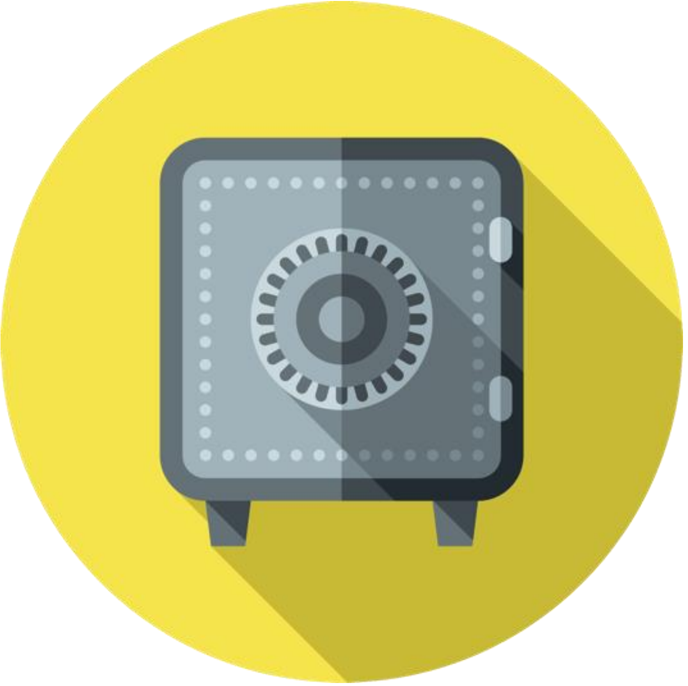
Welcome to the Chatroom.

I can't wait to meet you in person. 8:45

GOODBYE! 8:50

User has signed off.

SAFE PASSWORDS



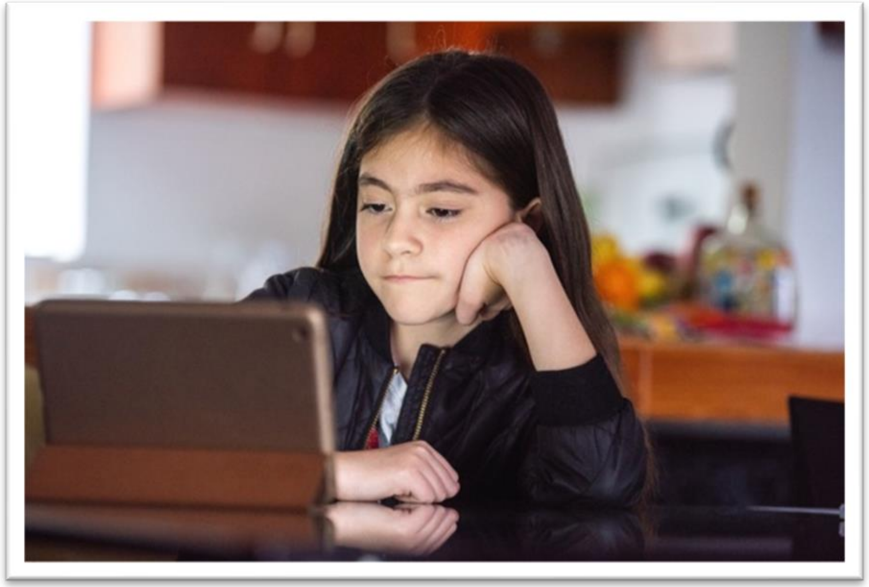
- Make it a phrase- the longer the better!
- 8 character minimum with no repetitive or sequential characters.
- No commonly used passwords and no context-specific words.
- Use a password vault to store all passwords safely.
- Use 2-Factor whenever offered.
- Make sure passwords are used on all mobile devices and computers.

DOWNLOADS

- Speak to your children about the risks of downloading.
- Make sure your antivirus software is updated.

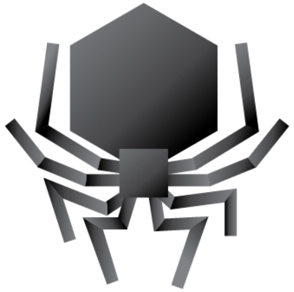
DOWNLOADS

- 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.

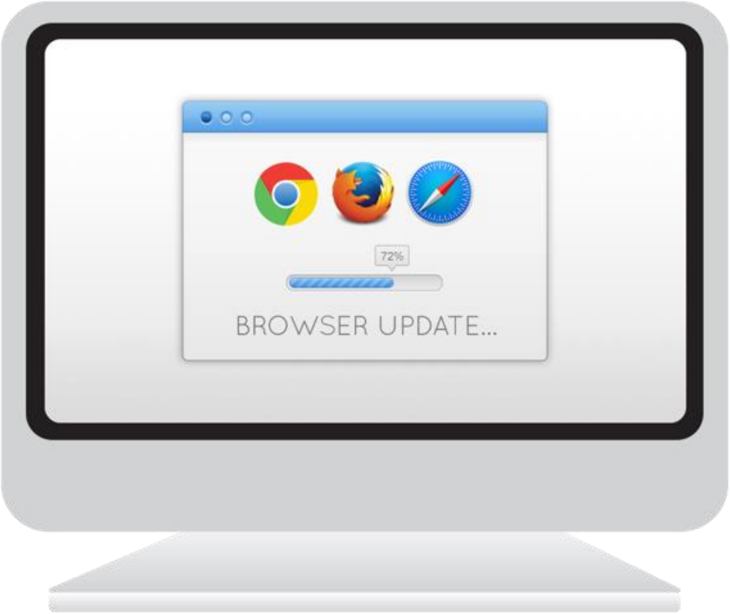
- Involve your children in the process so they understand what is protecting them and why.

BASIC PRECAUTIONS

"Antivirus software is the moat that protects our castle."

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.

- Teach your kids how to recognize phishing emails.
- Be cautious of attachments and links from any email. Always get confirmation from the sender first.

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

- Explain Sexting and Consequences
- Protect, Update, and Backup
- Know the Signs of Cyberbullying
- Monitor and Communicate

www.IAmCyberSafe.org

@IAmCyberSafe

@IAmCyberSafe

@Center for Cyber Safety and Education

@ISC2Cares