



JEFFERSON
COUNTY
SHERIFF'S
OFFICE

CHEEZO
TECHNOLOGY
SAFETY

www.Cheezo.org



CHEEZO

200 Jefferson County Parkway
Golden, Colorado 80401

www.cheezo.org

720-497-7278

RESOURCES

CBI Sex Offender Registry—Convicted Sex Offender Site:
<http://sor.state.co.us>

National Center for Missing and Exploited Children:
www.missingkids.com

National Center for Missing and Exploited Children
CyberTipLine:
Report.cybertip.org

National Center for Missing and Exploited Children
Content Removal
<https://www.missingkids.org/gethelpnow/isyoudexplicitcontentoutthere>

National Center for Missing and Exploited Children
TeamHOPE
<https://www.missingkids.org/gethelpnow/support/teamhope>

The Online Safety Project:
www.safekids.com

Netsmartz:
www.netsmartz.org

Common Sense Media:
Commonsensemedia.org

Protect Young Eyes:
Protectyoungeyes.com

PARENTS NEED TO KNOW

Some adults use technology to contact and lure children for sexual purposes. If an adult is communicating with a child through technology and asks, attempts to ask, says, or does the following, they have committed a crime:

- Ask anyone under the age of eighteen (18) for their naked or partially naked picture.
- An adult sending their naked picture or picture of their private parts to anyone under the age of fifteen (15).
- An adult communicating with anyone under the age of fifteen (15) about meeting them for sex or sexual contact is a felony, even if a meeting does not occur.
- An adult meeting anyone under the age of fifteen (15) for sex.
- There are many other things that can be illegal for an adult communicating with someone under the age of eighteen (18). If unsure we encourage you to contact law enforcement.

WHAT TO DO?

If you suspect that your child is communicating with a predator through technology, even if it hasn't escalated to the points listed above, consider the following steps:

- **Stop the communications immediately and take all technology away from the child until law enforcement is contacted.**
- **Do not contact the suspect or allow them to know parents are aware of the communications.**
- **Note the location where the communications are taking place, such as Facebook, text messaging, apps, or gaming sites.**
- **Save, screen capture, or print out the communications and/or pictures.**
- **Obtain your child's password for signing onto their device.**
- **Obtain your child's user name, email, or screen name, along with the password for signing onto the site they are communicating.**
- **Note the user name, email, or screen name of the person communicating with your child.**

CHILD SEX OFFENDER INTERNET INVESTIGATIONS

- The CHEEZO investigative team was the first in Colorado, and one of the first in the United States, to proactively seek out online predators. They divide their time between online investigations and presenting safety and educational programs to parents and children in the community.
- CHEEZO is proud of the technology safety programs presented to schools, parent groups, and other organizations. CHEEZO has presented more than 3,500 times to children and adults. There is no charge for presentations or appearances.
- The CHEEZO team goes undercover, following sex offenders into areas on the Internet frequented by children. As of 2022, they have made more than 1,240 arrests.
- If someone sends your child an inappropriate message or picture, contact your local law enforcement agency. Remember to save all of the messages and photographs for law enforcement to review. Even if a crime has not yet occurred, alarming communications should be reported to law enforcement.
- It is illegal for an adult to engage in sexual talk with a child under the age of 15 and/or talk about meeting a child for sexual purposes by email, text messaging or online in chat rooms, social networking, or gaming sites.
- It is illegal for an adult to send naked pictures of themselves to a child under the age of 15 using cell phones or personal computers, email, text messaging, or online in chat rooms, social networking or gaming sites.
- It is illegal for an adult to ask a child under the age of 18 for their naked pictures by email, text messaging, or online in chat rooms, games, or social networking sites.

TOOLS FOR PARENTS

Activities that may seem fairly harmless to your child can lure the many dangers of technology. There are some precautions your child can take, along with your help, that may help them be safe with technology.

SET LIMITS

Different ages, maturity levels, and special circumstances dictate what is appropriate for each child. Banning children from certain sites may motivate them to sneak time on those sites. The most important thing parents can do is stay involved with their children.

- Limit device usage to a well-trafficked area in your home. Consider having your child check in their devices at a certain time at night away from their bedrooms.
- Schedule times when a child can be on technology.
- Insist on access (including passwords) to social networks, email, gaming, and devices. Monitor periodically.
- Watch for changes in your child's relationships with adults. Adults who work with children have professional boundaries; cultivating significant technological relationships with individual children is not appropriate.

TIPS FOR CHILDREN

Children need to know that anything they post can be saved. Viewers can screenshot, save, distribute, or text photos. This means sexual images, photos depicting drug use, gang signs, threats, or criminal behavior are all potentially permanent for their classmates, friends, enemies, parents, and strangers.

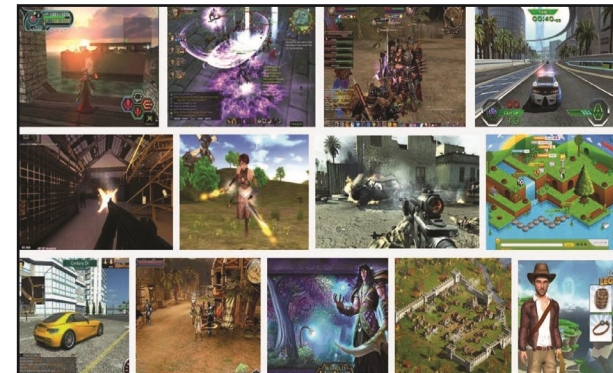
- The images, opinions, and personal information shared can be used by others to manipulate, blackmail, or physically locate a person. Choose a neutral profile photo that doesn't show faces. Consider an image of an object or landscape.
- Never take nude or semi-nude photos of yourself or allow someone else to do so.
- Never give out names, addresses, phone numbers, or school information.
- Select gender-neutral and age-appropriate screen names. You can inadvertently give out unwanted information with a screen name like "britt03" (Brittany, born in 2003). Screen names that suggest sex, violence, or drugs, which might seem fun, can draw attention from the wrong people.
- Lock down your privacy settings so only approved friends can see photos, video, and updates.

FACE-TO-FACE

Our most important message for children communicating with technology (computer, cell phone, tablet, iPad, or gaming device) is to only talk with people they know face-to-face.



GAMING



Many children play online games. Parents need to have rules in place if their child plays interactive online games where players communicate with each other in real-time while playing the games.

We have a simple rule: **“Play the Game, Don't Give Out Your Name”**. You can talk about the game, but not about “you”. Never give out your personal information when you are gaming. Personal information includes where you go to school, where you live, what sports you play, hobbies you have, or what you do for fun.

A TRUE STORY

Never assume that anything you send or post online is private.

A 16-year-old girl was asked by her 17-year-old boyfriend to send him a naked picture of herself. She felt pressured by her boyfriend to send the picture but she reluctantly did it. She took a picture of herself with her cell phone and then sent it to him in a text message.

The teen asked her boyfriend not to show it to anyone. He promised the pictures were just for him and that he would not show them to anyone.

Approximately two hours later the boyfriend sent the naked picture of his girlfriend to his best friend and told him not to show it to anyone else. The best friend also promised not to show it to anyone else.

Ten days later this 16-year-old went to school and found the naked picture she had sent her boyfriend taped to her locker. The same naked photo was also found taped in ten other places around the school.

The 16-year-old was humiliated and embarrassed. She was taunted and ridiculed. She was so devastated that she ultimately dropped out of school.

The two teenage boys responsible for this were charged with Sexual Exploitation of a Child. They were adjudicated and now have to register as sex offenders until they are both 26 years old. The 16-year-old girl was also charged and given deferred adjudication.

Sexting can be devastating and your children need to know how seriously it can affect their lives.

Once you post a photo online or send one through in a text message, that photo is in cyberspace forever.

- Only accept friend requests from people you know, trust, and meet with face to face.
- If you are contacted, in any format, by someone you don't know, do not respond. Use your settings to block that person from contacting you.
- **Never agree to meet someone in person who you met through technology. If you're contacted by an adult you know, talk to your parents about the communication.**

INSTALL SAFETY SOFTWARE

Software is an effective way to filter dangerous content. This software usually comes with tools like time management, remote monitoring and reporting, and keystroke recognition. Check with your Internet Service Provider (ISP). Some ISPs have filters you can purchase or they may provide filters for free. Visit a local electronics or computer store to examine and purchase a filtering software program or research and order a filtering software package. There are safety features available for cell phones as well, such as phonesheriff.com.

FOSTER OPEN COMMUNICATION

Open communication and trust are key. If your child comes to you about stumbling upon pornography or being approached by a stranger, they should be applauded. Many parents overreact out of fear and love. They tell their child they cannot go to that specific site or prohibit technology use altogether. That defeats all trust and closes the door to communication. After all, tech-savvy children can easily delete incoming text messages and images. Parents must be vigilant.

- You may control your child's environment at home, but when they are away from home someone else might not share your same rules and concerns. Set guidelines as well as consequences.
- Make sure you are clear with your children about what you consider appropriate technology behavior. Just as certain clothing is probably off-limits and certain language is unacceptable in your house, let your children know what is and is not allowed with technology.
- Make sure your children understand that messages and pictures they send are not private or anonymous and could be shared with school administrators and potential employers. Also, ensure they understand the short-term and long-term consequences of their actions.
- Teach your child that if they encounter pornography to quickly power off and get an adult. This can prevent a child from attempting to stop the situation by clicking more buttons and thereby spreading the attack. Talk with your child about the dangers of pornography. Pornography addiction can be just as dangerous as an addiction to drugs.

TECHNOLOGY SAFETY: Pictures and Personal Information

- The most important message the Sheriff's Office wants to relay to children is if you don't know someone in real life you should not communicate with them.
- Personal information posted online by a child can help a stranger find them. It takes very little personal information for someone to find out where a child lives, goes to school, or spends their free time.
- Personal information can include names, addresses, phone numbers, schools, hobbies, clubs, sports, or other activities in which a child might be involved.
- Pictures are also personal information. A picture of a child can assist a stranger in finding them.
- Once a child sends their picture to someone or a website, either online using their computer or a cell phone, it is gone forever. This is the same for written communication.
- All account settings for children, including teens, should be set to private.
- Parents should limit the number of "friends" with access to their child's accounts. The information posted by their child should be viewed only by those they know in day-to-day life.
- Many children have up to 500 "friends" on their social networking sites like Facebook, Instagram, or Snap Chat. This means that they do not know everyone face to face and that they could inadvertently have a predator as a listed friend.



KEEPSAFE

This free app is a storage center for photos that users want to hide. KeepSafe requires a password. One of the most important things CHEEZO tells children is "If you have to hide it, don't take it." While children desire the freedom to make their own online decisions, parents recognize this can put them in danger.

ASK.FM

Ask.fm is a question-and-answer format in which users interact by inviting others to ask or answer anonymous questions. Ask.fm is a foreign-based site that offers an anonymous channel for teens to communicate with friends or strangers without their parent's knowledge. When a user registers, they are provided a URL that can be copied to a teen's Facebook or Instagram page, providing direct anonymous access to unsuspecting teens. In addition, upon registering, extensive personal information is published on the site. Anyone signed up can see the information, including photos or videos, making Ask.fm a likely tool for child predators.

VIDEO GAMES

Many children and teenagers frequent popular game sites online such as Minecraft and Roblox. Many of these sites allow users to communicate with others who are also playing online. We tell children and teenagers that if they choose to communicate with others, talk only about the game. If someone asks how old you are, your name, where you live, or any other personal information, children should reply that they are only wanting to play the game.



TECHNOLOGY TRENDS AND APPS

Attractive new mobile apps and social networking sites are part of today's technology, but some apps pose significant risks to children. Unsuspecting teens can be exposed to malicious, anonymous postings including cyberbullying, sextortion, or pornography.

CHEEZO suggests parents take time to regularly review their child's electronic devices and familiarize themselves with the apps being used. Apps requiring a password are a red flag that may require further action.

Below are some of the latest technology trends and apps that CHEEZO has encountered in Jefferson County.

ENABLING TEXTING ON OLD DEVICES

Many parents are surprised to find their children can turn older devices into a texting instruments by downloading free applications like Text Free, text-Plus, or Text Now.

Even parents who are vigilant in checking their teen's cell phone messages sometimes are unaware their teen is texting from free applications on other devices. New applications come out every day and teenagers generally find and use them before we even know they exist. It's good practice to not only check the messages on your teenager's phone but all applications.

LOCATION SERVICES

Smartphones and digital cameras have location services through a global positioning satellite (GPS) feature that makes geotagging possible by providing latitude and longitude coordinates. After posting media, geotagging can share your exact home address, school address, work address, and places you frequent with strangers. You can turn off location services completely, or on an app-to-app basis.

Each time a new app is added, you should check to ensure the location services setting is turned off for that app. CHEEZO recommends disabling location services for your cell phone camera and most location services except maps and weather.

STRANGER DANGER—INTERNET STRANGER

In recent years we've seen an increase in the number of children approached by online predators in Jefferson County and throughout Colorado. Some of these children have been sexually assaulted by these sex offenders.

Parents are often shocked to find that their child has been communicating with a sex offender. Some parents believe their children are safe if they do not have internet access in their homes. Unfortunately, children are very resourceful and technologically savvy. They may use the internet at their friends' homes or at school. Today, most children have smartphones; they take Internet access with them wherever they go.

The Sheriff's Office CHEEZO Unit takes a dual approach to protect children online. While we aggressively pursue those who lure children on the internet, we believe we are more effective in presenting our technology safety programs to children, parents, and teachers. Parents and teachers have done a great job educating children about meeting strangers on the street. The CHEEZO team continues to stress the danger of those strangers, but also educates children about strangers met through technological means.

The CHEEZO Unit has developed a program called "Stranger Danger—Internet Stranger" targeting elementary school children. CHEEZO Believes that these younger children, first through third grade, are the ones who are most likely to make inadvertent mistakes online. The CHEEZO Unit still provides technology safety education for fourth-grade through high school students but believes they have a better chance of instilling lasting safety messages in the younger students.

This program has been extremely successful and has great reviews with a long lasting impression on the children and parents. The internet and advances in technology are here to stay. We encourage parents to attend a presentation so they can see this message and continue the dialogue.



DANGERS OF TECHNOLOGY

CHILD PREDATORS

The anonymity of technology allows predators to alter their personas. In one instance in Jefferson County, CHEEZO posed as a young girl and received a series of messages from a supposed 17-year-old boy. His language and the topics he discussed were convincing. When he attempted to set up a meeting with the girl, the Investigator's suspicions were confirmed; the "boy" was a 60-year-old convicted sex offender.

THREATS

The Sheriff's Office has investigated cases involving threats made through technology. In one case, a local boy posted photos of himself with his parents' gun collection. Classmates reported that he had made threats. Investigators arrested the boy and charged him with unlawful possession of a handgun by a juvenile.

CONSEQUENCES OF SEXTING

There are criminal implications for adults or children who possess sexual images or videos of young people. If you obtain the content from someone other than the original sender or forward the content to others, you could be charged with sexual exploitation of a child.

IDENTITY THEFT & BURGLARY

Sharing too much personal information, such as full name and date of birth, may allow a criminal to steal identities. Technology such as Google Street View, Facebook, Twitter, and Foursquare are being used by burglars to target homes and businesses.

PORNOGRAPHY

There is a massive amount of pornography available. Children with access to porn may develop an unhealthy concept of sex. Extremes in sexual behavior depicted, or the sheer volume of images can consume a child until reality becomes a distant memory. Porn addiction, sexual aggression, and violence toward women can develop from unrestricted access to porn.

SHARING PHOTOS

Sexting is the act of taking and sending sexually explicit photos electronically. This is a serious challenge facing children today. Young people fail to recognize the danger of sending intimate photos electronically. Photos are easily shared but impossible to retract. In addition to having potentially destructive social and legal consequences, sexting is a crime and may be the most under-reported criminal activity among teens.

Taking a naked selfie and sharing it with one friend may seem harmless; however, these photos are often shared with friends and friends of friends or may be posted on social media. The teen in the photo has no control over who sees the photo or where it may end up. Sexting can haunt them later in life by resurfacing during a college or employment application process.

SEXTING

The current law is designed for charging sexual predators, not children engaged in sexting. Children never think the trusted friend or boyfriend/girlfriend to whom the explicit photos were sent would ever pass them on, but they do. Once photos are sent from a cell phone they are not retrievable from cyberspace. Even deleting the photo or video may not be enough.

Sexting is illegal if the photographed person is under 18 years of age. It is illegal to possess naked pictures, and an even more serious offense is to send them or post them online. Sexting can result in criminal charges and sex offender registration.

SEXTORTION

Many teenagers take sexually explicit or even nude pictures of themselves and send them to others either online or through text messaging. These photos become sextortion when they are used as a tool of exploitation or extortion.

Recently a Colorado teenage girl made the mistake of sending a naked picture of herself to a 20-year-old man in California. The girl thought this young man liked her and she had feelings for him. She accepted him as a friend on Facebook. After receiving the teenage girl's naked picture, the man threatened her, telling her that if she didn't send him \$1,500 or send him more naked pictures of herself, he would send her naked pictures to all her friends on Facebook.

The teenage girl was faced with the possibility of her naked picture being distributed to all her friends and felt pressured to comply. She finally told her mother, who then alerted law enforcement. This 20-year-old man was identified, prosecuted, and sentenced to prison.

Sextortion cases are very concerning to law enforcement because frightened victims might give in to demands such as posing for explicit photos, having sex with the perpetrator, or sending them money. CHEEZO asks parents and possible victims of sextortion to report incidents to law enforcement immediately.