

ONLINE SAFETY

FOR PARENTS



OFFICE OF THE ARIZONA
ATTORNEY GENERAL

Mark Brnovich

www.azag.gov

2005 N Central Ave
Phoenix, AZ 85004

602.542.5025

400 W Congress
South Building, Ste. 315
Tucson, AZ 85701

520.628.6504

Outside Phoenix
or Tucson
Metro Area:

800.352.8431

An Internet Safety Message from Attorney General Mark Brnovich:

As a parent, you want to be aware of the potential dangers to your child. Of course, you do everything in your power to keep them safe. I have two daughters of my own and their well-being is my top priority. The Arizona Attorney General's Office takes the lead in prosecuting many predators who attempt to harm the public. These unsavory folks come in many forms; some of them are easy to recognize while others can be more difficult to detect, especially online.

While the Internet is incredibly useful, in the hand of a cyber-predator it can become a weapon. Whether you encounter sexual cyber-predators, cyber-bullies, "sexting" or an array of other misguided behavior, the power of the Internet to inflict damage on someone, especially a child, is significant.

It is important that parents recognize the risks that can be associated with social networking and Internet usage.

The Arizona Attorney General's Office provides a number of resources to help parents understand the dangerous aspects of the Internet; this booklet is just one of them. If you would like more information, please visit the Attorney General's website at: www.azag.gov.

Thank you,
Mark Brnovich
Arizona Attorney General



Mark Brnovich
Arizona Attorney General

TABLE OF CONTENTS

Arizona ICAC.....	4
Cyber Predators	8
The Grooming Process	9
Spotting the Warning Signs.....	10
Sexting	16
Cyberbullying	20
Online Safety.....	24
Know the Apps.....	27
Internet Safety Tools for Parents.....	30
Tips for Parents and Teachers	34
Resources	35



AZ ICAC TASK FORCE

The Internet Crimes Against Children Task Force program helps state and local law enforcement agencies develop an effective response to cyber enticement and child exploitation cases. This help encompasses forensic and investigative components, training and technical assistance, victim services, community education, and criminal prosecution.

Launched in 1998, the Internet Crimes Against Children Task Force (ICAC Program), started with only 10 task forces across the United States, but today it is a network of

61 coordinated task forces representing more than 3,000 federal, state and local law enforcement and prosecutorial agencies. These agencies are engaged in reactive, proactive, and forensic investigations, and criminal prosecutions.

By helping state and local agencies to develop effective, sustainable responses to online child victimization and child pornography, the U.S. Department of Justice, Office of Juvenile Justice and Delinquency Prevention has increased their capacity to address Internet crimes against children.



The Arizona Internet Crimes Against Children Task Force is comprised from city, county, state, and federal agencies, including the Arizona Attorney General's Office. Special emphasis is placed on locating, prosecuting, and imprisoning people who intentionally exploit children. The AZICAC Task Force diligently pushes to fulfill this goal with highly trained and professional investigators and cutting edge forensics and technology.

It is very important for parents to monitor their children on any device that connects to the Internet, (i.e. not just computers, but cell phones and other devices). By visiting resources on websites like www.azag.gov and www.azicac.org that contain educational videos for children, parents can educate themselves on child predators and learn additional ways to report abuse. Please review www.azicac.org for further information.

FROM THE CASE FILES OF AZ ICAC



25-YEAR-OLD SEEKS RELATIONSHIP WITH HIGH SCHOOLER

In one of the cases AZICAC prosecuted, a female high school student in Scottsdale, AZ, contacted school officials and police when a 25-year-old sexual predator stalked and followed the teen girl to her school and onto the school campus. She became frightened because she didn't think this would happen or that he would go to this extreme. The Arizona Internet Crimes

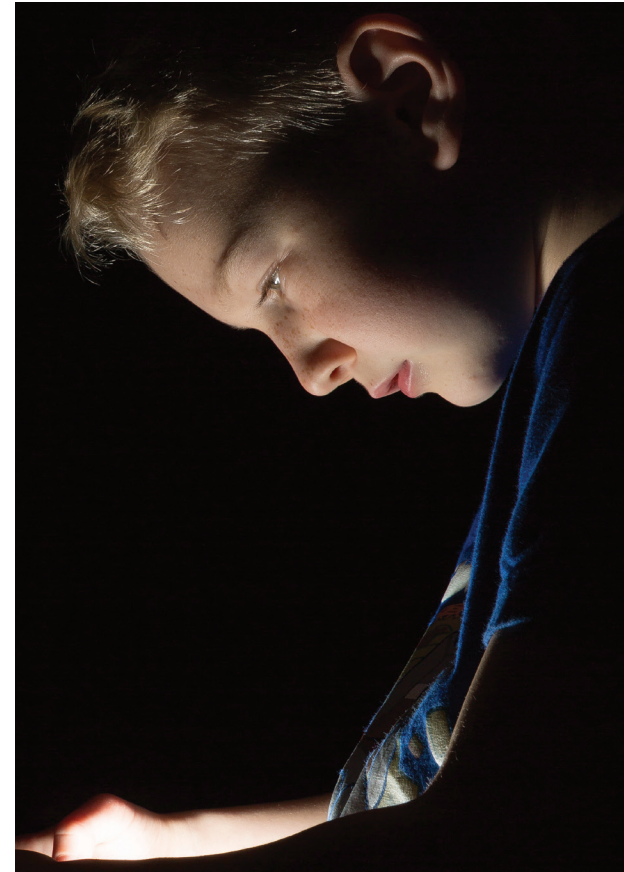
Against Children Task Force and Scottsdale Police arrested the man on school grounds. When the sexual predator was interviewed, he told police he met the girl online which led to an online relationship and eventually to him asking her to meet him in person. The victim had pornographic images sent to her by the predator which she provided to the police. The unemployed Scottsdale man was booked into Madison Street Jail and charged with luring a minor for sexual exploitation and furnishing harmful items to a minor via the Internet.

CYBER PREDATORS

Cyber predators seek to entice kids and teens via online platforms ranging from chat rooms, social media sites and video games. Cyber predators can be men or women, and come from all age brackets, including teens and young adults.

Cyber predators pay close attention to what the youth they are talking to are saying. Within 45 minutes they can usually find out where the child lives, attends school, and what their hobbies are.

Cyber predators are more likely to use sites and apps that offer anonymity such as messaging apps, text messages and live stream sites.



PREDATORS

WHO ARE CYBER PREDATORS?

- They may have a successful career
- They may be married with children of their own
- They may have no criminal history or none related to sex crimes
- Most are male, white and older than 26
- They may be perceived as “the last person you would expect to be a predator”
- They may not always lie about their age
- They search for potential victims for “grooming”
- They may engage in “sextortion”

WHO DO CYBER PREDATORS TARGET?

ANYBODY! Specifically:

- Kids/teens living in single-parent household
- Kids/teens with self-esteem problems
- Kids/teens who don’t communicate with their parents
- Kids/teens who are constantly online
- Kids/teens who are in foster care
- Kids/teens who are new to online activity
- Kids/teens who are attracted by subcultures apart from their parents’ world

REF: Janis Wolak, Kimberly Mitchell, and David Finkelhor, Online Victimization of Youth: Five years later (2006). Crimes Against Children Research Center, University of New Hampshire.
“The Facts About Online Predators Ever Parent Should Know,” Commensense.org, Christine Elgersma, July 2017

GROOMING PROCESS

The grooming process begins when a cyber predator looks for information regarding your child on their social media, chat and video game profiles. If your child’s profile is set to “public,” their pictures, location and likes are easily accessible.

Cyber predators will study the profiles to see if they can use information such as “shared” interests that they will use to start a conversation with your child. The cyber predator will then request to follow your child on social media, chat or online gaming profile.

Once the request has been accepted, the cyber predator will begin messaging the kid/teen with the goal of establishing a trust and filling a need, this is known as the “grooming process.”

The anonymity of the Internet makes it easy for cyber predators to lie about their identity and what their intentions are. Often, they will ask to move conversations from one online platform to another to maintain secrecy.

If a kid/teen shares a compromising picture with the cyber predator, a predator may engage in “sextortion.” The cyber predator demands more pictures and/or contact under threat of exposure or harm.

They will ask your child to keep the relationship secret. The ultimate goal is to meet face-to-face.



CYBER PREDATOR CHARACTERISTICS

1. TARGET
2. GAIN TRUST & INFORMATION
3. FILL A NEED
4. ISOLATE
5. THREATEN
6. MAINTAIN CONTROL

SPOTTING THE WARNING SIGNS

1. Your child becomes withdrawn and isolates themselves more often.
If it's child pornography, **SAVE THE IMAGE BUT DO NOT PRINT OR SEND!! CONTACT POLICE IMMEDIATELY!**
2. Your child is spending more time online. Ask what is causing them to spend a significant amount of time online. Use your web browser's "Internet History" to view previously visited websites.
3. Your child turns off the screen or locks their electronic device when you walk in the room. Talk to them about their online activity. Be aware that prying too much could foster paranoia and lead to more secretive behavior and further isolation.
4. You find sexually explicit content/ pornography on the computer. If it's adult pornography discuss it with your child.
5. Your phone bill has calls to unknown numbers. Do a reverse phone directory search online to find out whose number it is.
6. Your child receives mail/gifts/packages from senders you don't know. Track the package. Use the same tools cyber predators use to get information, such as reverse address directory searches, email address searches, Google searches, etc. Once the relationship reaches this level, it's time to intervene.
7. Your child talks about a friend you don't know or an older "boyfriend/girlfriend."

ONLINE ENTICEMENT

Online enticement is when a child is being groomed through an online "relationship" by a cyber predator. A child who is experiencing online enticement may be:

- Spending a significant amount of time online
- Becomes upset when they are not allowed on their device
- Taking extra steps to conceal what they are doing online
- Receiving gifts from people you do not know

If your child or someone you know has been victimized by someone they met online, report them to your local police department and to www.CyberTipline.com.



PROFILES & PRIVACY

1. KNOW THE PLATFORMS

Cyber predators operate on all platforms including websites, online gaming services and apps.

2. BE PROACTIVE

Talk to your kids about the common tricks used by cyber predators.

3. FILLING OUT ONLINE PROFILES

Users should abstain from filling out all of the profile questions. Oversharing information will allow cyber predators to “find” your child in real life.

4. ENGAGE

Talk to your children about Internet use and protecting themselves online. Let them know public profiles of people they are communicating with might not always be that person.

5. DOWNLOADING PICTURES FROM AN UNKNOWN SOURCE

Downloading a picture may bring hidden viruses, which may destroy your computer, or place ‘cookies’ that allow the sender to track sites you and your child visit, as well as keystroke trackers that may be used to steal your child’s identity.

6. POSTING PICTURES ON THE INTERNET

Digital photos of your children could be spread all over the Internet, or your child could be blackmailed into sending more photos.

7. USING A WEBCAM

For a cyber predator, a webcam is the next best thing to an in-person meeting. Cyber predators will use what they see to take advantage of your child. They may record the video chat and post it for others to see or simply wait and use it against your child later.

8. ACCEPTING WEBCAM VIEWS FROM STRANGERS

By accepting an invitation to video chat from strangers, your child could be exposed to nudity and sexually explicit material. Ask your child never to accept a webcam invitation from a stranger or click a link in a chat room.


9. ARRANGING AN IN-PERSON MEETING WITH SOMEONE MET ONLINE

Your child could be hurt, assaulted, kidnapped or worse, during an in-person encounter.

10. SPOT THE RED FLAGS

Learn about the signs your child may unconsciously give you if they are experiencing online enticement.





SO, HOW OFTEN ARE YOUTH RECEIVING UNWANTED SOLICITATIONS ONLINE?

1 IN 9

youth experience online
sexual solicitation.

1 IN 5

youth experience unwanted
online exposure to sexually
explicit material.

REF: Madigan, S. et. al, "The Prevalence of Unwanted Online Sexual Exposure & Solicitation Amount Youth: A Meta-Analysis," Journal of Adolescent Health, June 16, 2018.





Sexting is the sending or distributing of nude or partially nude images over an electronic device usually sent between cell phones; sexting can also occur over computers and tablets.

Many teens enjoy the privacy and freedom cell phones provide them, but what happens if your child begins to participate in sexting?

TALKING TO YOUR TEEN ABOUT SEXTING

THE RISKS

Teens who take, send or forward sexting images may face:

- Embarrassment if their picture is spread and is seen by friends, family, classmates and even strangers
- Bullying or harassment from peers who judge them for sexting
- Termination from school sponsored activities, i.e., sports teams, clubs
- School suspension or expulsion
- Future consequences with college admission offices
- Future consequences with future employers
- Criminal charges
- Fines of up to \$150,000

HOW TO TALK ABOUT SEXTING

- **Ask questions** to make it clear that you are comfortable discussing it
- **Discuss** what characterizes a healthy relationship
- **Explain** how quickly images can be spread online and through mobile devices
- **Make clear** once you post or send an image it never truly goes away
- **Emphasize** the importance of not forwarding sexts they receive
- **Always report** sexually explicit images



IF YOUR CHILD'S IMAGE IS ALREADY OUT THERE

- Help them report it to the website(s)/ app(s) where the image is posted
- Make it clear your child is a minor and the image was posted without his/her consent
- Talk to school officials so they can help stop the spread of the image and any harassment that may be happening
- Contact police if your child's image was shared or forwarded, or if your child is being blackmailed, harassed or if it involves an adult
- Consider seeking professional counseling, if needed
- Offer support

RESOURCES



CYBER-BULLYING

Cyberbullying occurs when bullying takes place using electronic devices and equipment such as cell phones, computers, and tablets

via social media sites, text messages, chat, websites and video games. A cyberbully's goal is to harass, threaten or intimidate their victims.

HOW IS CYBERBULLYING DIFFERENT THAN BULLYING?

Kids who are being cyberbullied are often being bullied in person too. The messages the cyberbullies are posting can be anonymous, and can be distributed and replicated quickly. Once the harassing messages are posted, they are nearly impossible to delete if they spread quickly.



CYBERBULLYING HAPPENS

24/7



KEEP THE EVIDENCE

SCREENSHOT SAVE PRINT

CALL THE POLICE
IF IT INVOLVES THREATS

IF YOUR CHILD IS RECEIVING
HARASSING MESSAGES, REPORT
THEM TO:



WHAT CAN YOU DO?

If your child is experiencing nightmares, avoiding school, or seems secluded, start a conversation with them about cyberbullying and whether they are experiencing it.

If they are a victim of cyberbullying, report the messages to the sites and school officials. Help your child block the sender. Save the harassing messages, and make a police report if needed.

CYBERBULLYING TACTICS

- Posting hurtful or harassing comments, rumors, pictures or videos online
- Threatening to hurt someone or telling someone to hurt themselves
- Pretending to be someone else online in order to solicit personal or false information about someone else
- Creating a webpage about someone
- Posting mean or hurtful names or content about race, religion, ethnicity, sexual orientation, or other personal characteristics



ONLINE SAFETY



For teens, it may be hard to tell where their online profiles start and end. Many use their various online social media accounts to express themselves in ways other

than how they would in real life. Through the increased time spent online, they may be exposed to misguided behaviors they otherwise would not encounter.

24%

of teens believe social media has had a negative effect on people their age

40%

of social media users say it would be hard to give up social media, a 12% increase since 2014

45%

of teens say they are online at a near-constant basis

38%

of teens believe social media has had a mostly positive effect on people their age

45%

of teens believe social media has had neither a positive or negative effect on people their age

REF: "Teens, Social Media & Technology 2018," Pew Research Center
"Teens, Technology and Friendships," Pew Research Center



SOCIAL MEDIA USAGE

In the past three years, Facebook usage among teens has decreased by 20%. Sites like YouTube, Instagram and Snapchat have increased in popularity with teenagers. The most commonly used apps by teenagers, in order of popularity, are YouTube, Instagram, Snapchat, Facebook, Twitter and Reddit.

An estimated 95% of teens have a smartphone or access to one, a 22% increase from the 73% reported in 2014-2015.

Unlike former years, social media usage doesn't revolve around only one site. Girls are more likely to use Snapchat while boys frequent YouTube or play online games.

KNOW THE APPS



Snapchat

Snapchat allows users to add friends, share stories with friends or everyone, and share location. Account can be private or public.



Twitter

Twitter allows users to post pictures, messages, a small bio, and location of a user. Account can be private or public.



Yubo/Yellow

Yubo/Yellow allows users to add friends around the world, chat, send and receive pictures, and go live with public livestreams accessible by all users.



Amino

Amino allows users to add friends around the world that share common interests, watch videos, and create blogs.



Secret Calculator

Secret Calculator allows users to hide images, videos and messages in an app disguised as a calculator. This is one of many hidden apps available.



HOLLA

HOLLA allows users to random video chat with other HOLLA users.



TikTok

TikTok (Musical.ly & Live.ly) is a livestreaming app. Users can add filters and music to their videos. Users can chat with friends or strangers who are watching their public streams.



Twitch

Twitch is a live streaming video platform. Users can view a variety of live stream content including users who live stream their daily life and gamers who stream while playing video games.



WhatsApp

WhatsApp allows users to chat, call and send or receive photos, videos and voice messages to any of your contacts. The user always stays signed in if the app is downloaded onto their cellphone.



Whisper

Whisper allows users to post and share photo and video messages anonymously.



Instagram

Instagram allows users to post pictures and stories to their accounts. Users can have public or private accounts.



Vora

Vora allows users to track how long they have been fasting. Users can link to other social media accounts or encourage others to keep fasting through the app.

ONLINE GAMING

Aside from social media sites, websites and chat rooms, teens are also being solicited through online gaming. Teens ages 13-17 are playing video games on a computer, game console or portable device. Online gaming is the only platform where the presence of teenage boys surpasses that of teenage girls.

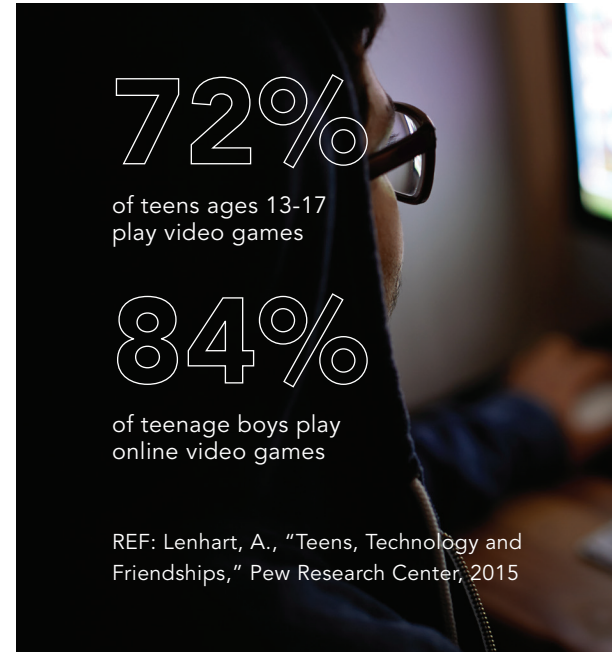
Boys are less likely to report or unfriend someone who they are not friends with, therefore, it is important to be aware of people

who try to communicate with your child via online gaming for reasons other than playing the game.

Gaming consoles allow users to place privacy settings on their accounts. As a parent, you can adjust the console privacy settings as you see fit.

Users are able to chat with other players whether they have been added as friends or strangers they meet while playing online. Talk to your child about not engaging in conversations with users they do not know, how to report users and how to block them if needed.

Aside from cyber predators who may attempt to engage in conversation with your child via chat, online users who are looking to scam other players will pretend to be game developers, for example, and ask for account passwords. Game developers will not ask for passwords. Fraudulent accounts will ask for passwords to access in-game purchases on the account and attempt to resell them for monetary gain.



REF: Lenhart, A., "Teens, Technology and Friendships," Pew Research Center, 2015

INTERNET SAFETY TOOLS FOR PARENTS

There are a number of tools parents can use to protect their children from Internet dangers. Although none of them are foolproof, they can help. Here are a few:

- **Computer Placement**

Keep the computer in a common area of your home.

- **Gaming Consoles**

Gaming consoles also include privacy and parental control settings. For more information about privacy settings and parental control settings, consult the console's help files.

- **Viewing Internet History**

To track your child's online activity, you can use the Internet history and temporary Internet files to see what websites have been accessed recently. For more information about viewing Internet history and temporary Internet files, consult your browser's help files.

- **Filtered ISPs**

Most Internet providers provide filtering and blocking tools to help protect your child online. Contact them for more information.

- **Software**

There are many software programs available for purchase. Some of the options these programs can give you include:

- Blocking chat rooms/instant message
- Blocking downloads
- Disabling links in chat rooms
- Allowing only approved addresses to email your child
- Filtering websites
- Filtering searches or allowing your child to use children safe search engines
- Recording chat room conversations or instant message conversations
- Notifying you by email when your child tries to access inappropriate websites
- Limiting the time spent online
- Allowing third-party rating of websites
- Recording key strokes

Not all these options are included in each software program. Each program is different. Compare and find the program that suits your needs.

- **User Profiles**

Every person who uses a shared computer in the home can have their own user profile. This allows you to set up different levels of access for each of the different users. To get more information about setting up user profiles, consult your computer's help files.

- **Web Browser Controls**

Most web browsers have a way to filter and block access to inappropriate websites. Web browser settings, used in conjunction with user profiles, fine tune the level of access different users have on the Internet. By fine tuning these controls, you can customize the type of content that each user can access. For more information on using these, settings, consult your browser's help files.



ONLINE LANGUAGE

As a parent you might not be familiar with the online language your children are using.

See how many of these common online acronyms and phrases you recognize.

Acronyms Every Parent Should Know	
BRB	Be right back
BTW	By the way
HMU	Hit me up
LOL	Laughing out loud
LMAO	Laughing my a** off
SMH	Shaking my head
WTF	What the f***
WYD	What you doing
WYA	Where you at
OOMF	One of my friends
POS	Parent over shoulder
AF	As f***
ASL	Age, Sex, Location

Words Every Parent Should Know	
Thirsty	Desperate, impatient, or overly eager
Shade	An insult, putting someone else down
Salty	Angry or bitter
Woke	Knowledgeable on current issues
High key	Making something known
Low key	Keeping something secret or being discrete
Sus	Suspicious

AGE-APPROPRIATE GUIDELINES

Teenagers are protective of their privacy and are least willing to share what they are doing online. They will probably tell you that they

don't want to be treated like a child. Keep this in mind when you create age appropriate Internet usage rules for your children.

Here are some general guidelines, although some may apply more to teenagers.

- Be skeptical about what you read on the Internet, especially from someone in a chat room. It's easy to lie online, and a cyber predator will tell as many lies as possible to gain your trust.
- Be careful about what information you give someone online, especially personal information that can be used to locate you.
- Do not download files an unknown sender has sent you. They can contain inappropriate material or viruses.
- Do not video chat with a stranger.
- Do not meet someone in person that you met online. Once your teenager has

obtained their driver's license or if they use public transportation, it can be difficult for you to prevent this from happening. You can emphasize how dangerous it is to meet someone you don't know alone. If you decide to allow them to meet someone from the Internet, they should be accompanied by an adult and meet in a public place.

- Be smart about what information you include in your online profiles. Don't include information that can be used to locate you. Remember to emphasize the importance of making online profiles private or for friends only.



PROTECTING YOUR KIDS ONLINE

SET GROUND RULES

Discuss the types of sites your child can visit, apps they can download, and appropriate electronics use.

RESEARCH BEFORE YOU BUY

Know the features of a device before you buy it. Will it allow unknown people to communicate with your child? Will this device allow your child to make unchecked purchases?

GO BEYOND SAFEGUARDS

Time, attention and active conversation are the best tools to help you and your child stay safe online.

**Remember, the Internet is here to stay.
It's our job to help our kids be Internet safe
and smart.**

INTERNET SURVIVAL TIPS FOR PARENTS AND TEACHERS

1. Be aware and involved.
2. Research the latest social media and gaming sites.
3. Talk to your kids.
4. Teach safety.
5. Set family online rules.
6. Report suspicious activity.
7. Help kids view online information with a mature point of view.
8. Be aware of your own online habits and set the example.
9. Make sure you keep channels of communication open.
10. Embrace their world.

RESOURCES

Arizona Attorney General's Office
www.azag.gov
Phoenix: 602.542.2123
Tucson: 520.628.6504
Outside the Phoenix or Tucson area:
800.352.8431

**Arizona Internet Crimes Against
Children Task Force**
www.azicac.org
623.466.1835

**National Center for Missing &
Exploited Children**
www.missingkids.com
CyberTipline
www.missingkids.com/cybertipline
1.800.THE.LOST | (1.800.843.5678)

**Federal Trade Commission
Consumer Information – Privacy,
Identity & Online Security**
<https://www.consumer.ftc.gov/topics/privacy-identity-online-security>

notMYkid – Internet Safety
www.notmykid.org/Internet-Safety/

Family Safe Computers
www.familysafecomputers.org

NetSmartz Workshop
www.netsmartz.org
www.netsmartz411.org

**State of Arizona Department
of Public Safety Sex Offender
InfoCenter**
[www.azdps.gov/services/sex_](http://www.azdps.gov/services/sex_offender)
[offender](http://www.azdps.gov/services/sex_offender)

Pew Research Center
www.pewresearch.org

**National Highway Traffic
Safety Administration**
www.nhtsa.gov
1.888.327.4236

**U.S. Department of Justice -
Office of Sex Offender Sentencing,
Monitoring, Apprehending,
Registering and Tracking –
Education & Prevention**
[https://www.nsopw.gov/en/](https://www.nsopw.gov/en/Education/FactsStatistics)
[Education/FactsStatistics](https://www.nsopw.gov/en/Education/FactsStatistics)

StopBullying
www.stopbullying.gov

Common Sense Media
[www.commonsensemedia.org/](http://www.commonsensemedia.org/parent-concerns)
[parent-concerns](http://www.commonsensemedia.org/parent-concerns)

The material in
this brochure is
not copyrighted.
We encourage
organizations to
reprint this booklet
or excerpts and
there is no need
to contact the
Arizona Attorney
General's Office
for permission.



COMMUNITY OUTREACH AND EDUCATION

The Arizona Attorney General's Community Outreach and Education Division is committed to educating Arizona residents about crime prevention. Community Outreach Coordinators are available to give educational presentations upon request to groups and communities

statewide. Additionally, we are available to distribute educational materials at local events. Our office operates a network of satellite offices, staffed by volunteers, throughout the state, making it easier for Arizona residents to gather information and remain educated

about the issues affecting them. Our goal is simple: preventing YOU from becoming a victim. Information about resources, satellite offices, and requesting presentations is available on the Attorney General's website azag.gov.

OTHER PUBLICATIONS AVAILABLE FROM THE ARIZONA ATTORNEY GENERAL'S OFFICE:

- Consumer Guide for Young Adults
- Human Trafficking
- Life Care Planning
- Senior Tool Kit
- Top Consumer Scams
- Suicide Prevention
- Opioid Awareness

FOR MORE INFORMATION, CONTACT:

Community Outreach and Education

Arizona Attorney General's Office
2005 N Central Avenue
Phoenix, AZ 85004
602.542.2123
communityservices@azag.gov



WWW.AZAG.GOV



AZAG_Outreach



AZAG_Outreach



AZAGOutreach

Special Thanks

Many individuals and groups helped make this Online Safety publication possible. We want to specially acknowledge the Arizona Internet Crimes Against Children (AZ ICAC) Task Force, The National Center for Missing and Exploited Children and NetSmartz Workshop, and the Pew Research Center. This project was supported with federal funds from the U.S. Department of Justice through a sub-grant from AZ ICAC, Phoenix Police Department.