

CU L8r

HOW SAFE
IS YOUR CHILD FROM
CYBER-SHARKS?

Tristram J. Coffin
United States Attorney
District of Vermont

internet safety guide
for parents



even **YOUR CHILD**
can become a target



Dear Parent,

The Internet is now a significant part of our daily lives. Social networking, smart phones, shopping, online gaming, chat rooms, banking and all kinds of daily tasks are now performed almost exclusively online. The Internet, in this role, has become a life line to our friends, family and the world.

Although the Internet is an important tool for us, it is far more than that for our children. Whether we like it or not, the Internet is a major component of their lives and is essential to how they interact with the world. As with all important technological advances, the Internet comes with risks. People intent on harming children have become masters at manipulating others through the use of the Internet, gaining access to and communicating with potential victims. Other children may use the Internet for electronic bullying and harassment that may be just as devastating. For our children to recognize and avoid these risks, they need to be made aware of them and given the tools to deal with them should they encounter them. If we enhance the critical thinking skills of our children, help them clearly articulate personal boundaries - whether online or offline - and nurture compassion for others, we will help our families detect unsafe situations and avoid hurting others.

Parents must be the first line of defense against online victimization. It is in this spirit that we enclose the first edition of the "Internet Safety Guide." I urge you to read this booklet carefully and to use it as a starting point for an ongoing conversation with your children about Internet safety. It will take a community-wide effort to safeguard our children. That effort will only be successful if all parents teach online safety at home, monitor their children's Internet activities, and talk openly with their children about the risks, even at a very young age. Your children are much less likely to be victimized if you're actively involved in their Internet lives, working with them to understand the risks and consequences.

I hope you find this booklet a helpful resource for beginning the discussion with your children.

Thank you,



Tristram J. Coffin
United States Attorney
District of Vermont



STEP UP: Protect Kids from Sexual Abuse
Website: <http://dcf.vermont.gov/stepup>
Child Abuse Hotline: 1-800-649-5285
Child Support Helpline: 1-800-786-3214

Safe at Home: Address Confidentiality Program
Website: <http://www.sec.state.vt.us/otherprg/safeathome/safeathome.html>

Phone:
802-828-0586 (voice and TTY)
1-800-439-8683 (Vermont only)

Vermont Internet Crimes against Children Task Force (VT-ICAC)
Website: <http://www.vtinternetcrimes.org/>
Phone: 802-540-2112

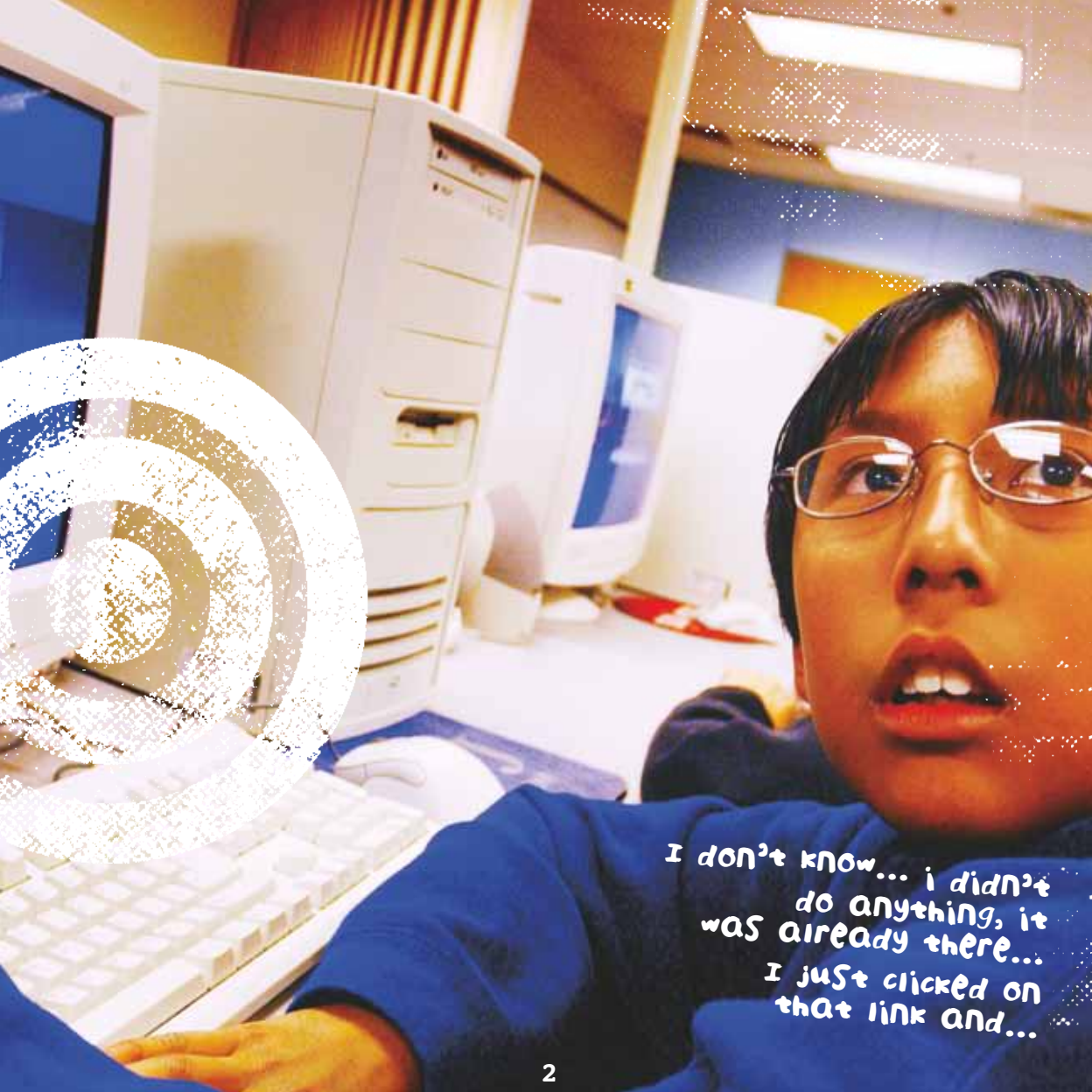
National Center for Missing and Exploited Children
Website: <http://www.missingkids.com>
24-hour Hotline: 1-800-THE-LOST (1-800-843-5678)
Phone: 703-224-2150

The Internet is a huge information source and it's a valuable tool for adults and children. However, because of its anonymous nature, it is also a breeding ground for abuses from childhood bullying to identity theft to sexual exploitation.


OFFLINE, a predator will often befriend the parents as well as the child, because the parents are the gatekeeper to the child.

ONLINE, there is no gatekeeper. Education is your greatest tool.

If you would like an Internet Safety presentation in your community or school, you can contact the office of the Attorney General at 1-802-828-3171 or your local sexual assault support center at 1-800-649-5285.



I don't know... i didn't
do anything, it
was already there...
I just clicked on
that link and...



hmm ...
but didn't he write he
just turned 20?! ...
it's a cute doggie he got
for me though...

THE PROBLEM IS SERIOUS:

- >>> 1 in 7 youth has been sexually solicited online
- >>> 1 in 3 youth has been exposed to sexually explicit pictures online without seeking or expecting them
- >>> 1 in 10 youth has met someone face to face they met online
- >>> 2 out of 5 youth trust the people they talk to on the Internet
- >>> More than 80 percent of youth spend at least an hour a day on the Internet
- >>> Today's youth use chat rooms and instant messaging as their primary means of communication

Cyber predators are tough to spot.

Who are cyber-predators?

Not who you think.

- They are likely to have above average intelligence and income
- 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"

WHO DO PREDATORS TARGET?

ANYBODY!

HOW DO THEY LURE CHILDREN?

- It usually begins in a chat room
- A predator pays close attention to what the child is saying - within 45 minutes they can determine where the child lives, goes to school, what they do for fun, what their real name is, and on and on
- The predator can move the chat from online to the phone and ultimately to a face-to-face meeting

Remember, being the target of a predator has nothing to do with intelligence, street savvy or even how much your child knows about the Internet. It can happen to anybody.

The search for the potential victim usually begins in a chat room, but your child might catch the attention of a predator from information they have provided on their blog or profile on a social networking site like myspace.com.

The predator looks for clues about the child: what they like to do, the type of music they listen to, what they do for fun, and how old they are. Much of this is often in the child's user name. A predator pays close attention to what the youth is saying in a chat room or what they have written and posted online.

The predator can then ask to be included on the child's "buddy list" and be able to tell every time the child is online. A buddy list is a feature that keeps the names and addresses of others who are contacted frequently in a chat room, somewhat like a chat room address book. When a user signs into an instant messenger service, their screen name will automatically appear in the "buddy list" of anyone else online who has saved their online ID as a "buddy." Communication can then begin instantly.

Anonymity online allows the predator to become a friend. In normal circumstances, your child would never develop a relationship with an older

person. But online, that predator can claim to be Prince or Princess Charming because it's easy to lie online.

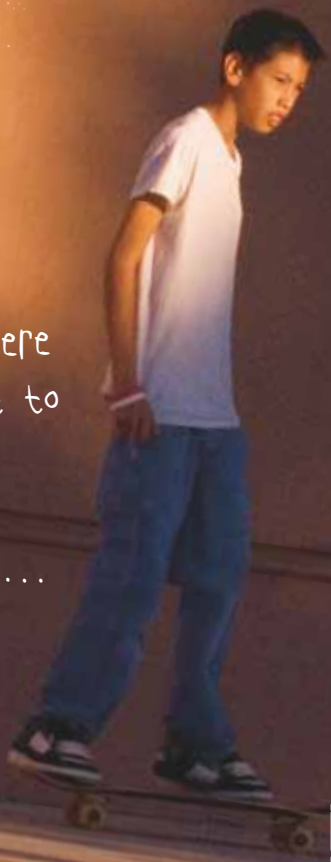
Over time, the predator can develop a relationship with the child and build trust with him/her. The predator will ask the child to keep their relationship secret. Later the predator can use the secrecy as a weapon against the child - threatening him/her with telling their parents or even harming the child if he/she tries to end the relationship.


IN REAL LIFE, a predator can befriend the parents as well as the child, because they are the gatekeeper to the child. ONLINE, there is no gatekeeper. Chat rooms that attract youth also attract predators.

At some point, the predator can move the relationship to the next phase. They can engage in phone calls with the child. The ultimate goal is to arrange a face-to-face meeting, frequently for the purpose of a sexual encounter, but sometimes the consequences are deadly.

PARKING
DELIVERIES
ONLY

the guy was supposed be here
already! I cannot wait to
get my new game...
I mean, how cool is
that: he just offered...




A young man with short dark hair and glasses is looking intently at a computer monitor. He is wearing a dark blue shirt. The background is slightly blurred, showing a desk with a keyboard and other computer equipment. A speech bubble is positioned near his mouth, and a large, stylized circular graphic with concentric rings is overlaid on the right side of the image.

BRB TAW...

As a parent, you're probably not up to date on the latest in **ONLINE LANGUAGE**. See how many of these common online acronyms you recognize:

1. ASL
2. POS
3. P911
4. BEG
5. FMTYEWTK
6. 121
7. KOL
8. MOTOS
9. WIBNI
10. LMIRL
11. SAW
12. TAW
13. WTGP

- 
1. AGE/SEX/LOCATION
 2. PARENT OVER SHOULDER
 3. PARENT ALERT
 4. BIG EVIL GRIN
 5. FAR MORE THAN YOU EVER WANTED TO KNOW
 6. ONE TO ONE
 7. KISS ON LIPS
 8. MEMBER OF THE OPPOSITE SEX
 9. WOULD'N T IT BE NICE IF...
 10. LET'S MEET IN REAL LIFE
 11. SIBLINGS ARE WATCHING
 12. TEACHERS ARE WATCHING
 13. WANT TO GO PRIVATE?

FMTYEWTK

Don't feel bad if you don't. A national survey showed that only between 4 and 8 percent of adults could correctly identify the acronyms.

Here's an EXAMPLE OF AN ONLINE CHAT that a child could experience and how it can move to the next level:

- A** Child starts chat, expresses feelings that the predator can easily pick up on.
- B** Predator begins "grooming" by expressing empathy to gain the child's trust.
- C** Child further expresses trust in the person he/she is chatting with, encouraging the predator.
- D** Further expression of empathy from predator.
- E** The child's frustration is evident to the predator who takes full advantage of the child by portraying himself as a trusted confidant.
- F** Predator offers a way to entice the child.
- G** Of course, there is no "rich uncle." The predator gives that impression to the child by waiting for a period of time before sending his next message.

- A** **CHILD:** my mom sux! its her falt that my parents are gettin divorced
- B** **PREDATOR:** i no. my parents r2.
CHILD: we never have \$\$ nemor (*"We never have money anymore."*)
CHILD: evry time i need sumtin she says the same thing "we cant aford it"
CHILD: when my parents were 2gether i could buy stuff
- C** **CHILD:** now i cant
- D** **PREDATOR:** me to. i hate dat.
CHILD: i w8ed 6 mos for this game to come out (*"I waited 6 months for this game to come out."*)
CHILD: my mom promisd me wed get it.
CHILD: can i get it now? nope.
CHILD: we dont have enuf \$\$\$.
- E** my mom sux!
PREDATOR: wow. dats tuf
- F** **PREDATOR:** i hav a realy cool uncle
PREDATOR: buys me things all the time
PREDATOR: he has lots o \$\$\$
CHILD: ur sooooo lucky!
PREDATOR: i got an idea. ill see if hell by it 4 u.
CHILD: really? thx man!
PREDATOR: brb gonna call him
- G** (*"Be right back. I'm going to call him."*)

PREDATOR: w00t! he said k **H**
CHILD: wow realy? thx i cant
bleve it.
PREDATOR: where do u live? **I**
CHILD: brlngtn, vt u?
("Burlington, Vermont. You?")
PREDATOR: georgia, vt uncle 2. ne
malls near u? *("Georgia, Vermont.
Uncle, too. Any malls near you?")* **J**
CHILD: university mall. **K**
PREDATOR: ive herd of that one.
Saturday ok?
CHILD: sounds good.
PREDATOR: b ther at 12 **L**
CHILD: k. meet at the game store.
PREDATOR: k!
CHILD: well g2g. thx again dude
*("Well, got to go.
Thanks again, dude!")*
CHILD: this is awesome!
CHILD: TTYL! *("Talk to you later!")* **M**
PREDATOR: l8r *("Later.")*

H Predator expresses excitement, tells the child the "uncle" will buy the game.

I Predator starts asking for clues about the child, begins the process of scheming to find out where the child is to arrange a face-to-face meeting.

J The predator will place himself in close proximity to the child, regardless of his actual location.

K Child has actually just determined the final meeting place without realizing the danger he/she is in, even though trust has been built up with the new "friend."

L Predator finalizes the meeting.

M The predator now has all the information he needs to meet the child face to face.

THE GROOMING PROCESS



WARNING SIGNS THAT YOUR CHILD
MIGHT BECOME A VICTIM AND
WHAT TO DO ABOUT IT



1. Your child becomes withdrawn from the family, isolates him or herself more often

Talk to your child, his/her teachers, consider counseling.

2. He/she is spending more time online

What is he/she doing that is causing them to spend so much time online? Research for school? Chats? Downloading? Games? Use your web browser's "Internet History" to view the websites that have been visited.

3. He/she turns off the screen when you walk in the room

What does your child not want you to see? Are they ashamed of something? Talk to them about their online activity. Be aware, though, that prying too much could foster paranoia in your child and lead him or her to more secretive behavior and greater isolation from you.

4. You find disturbing pictures on the computer

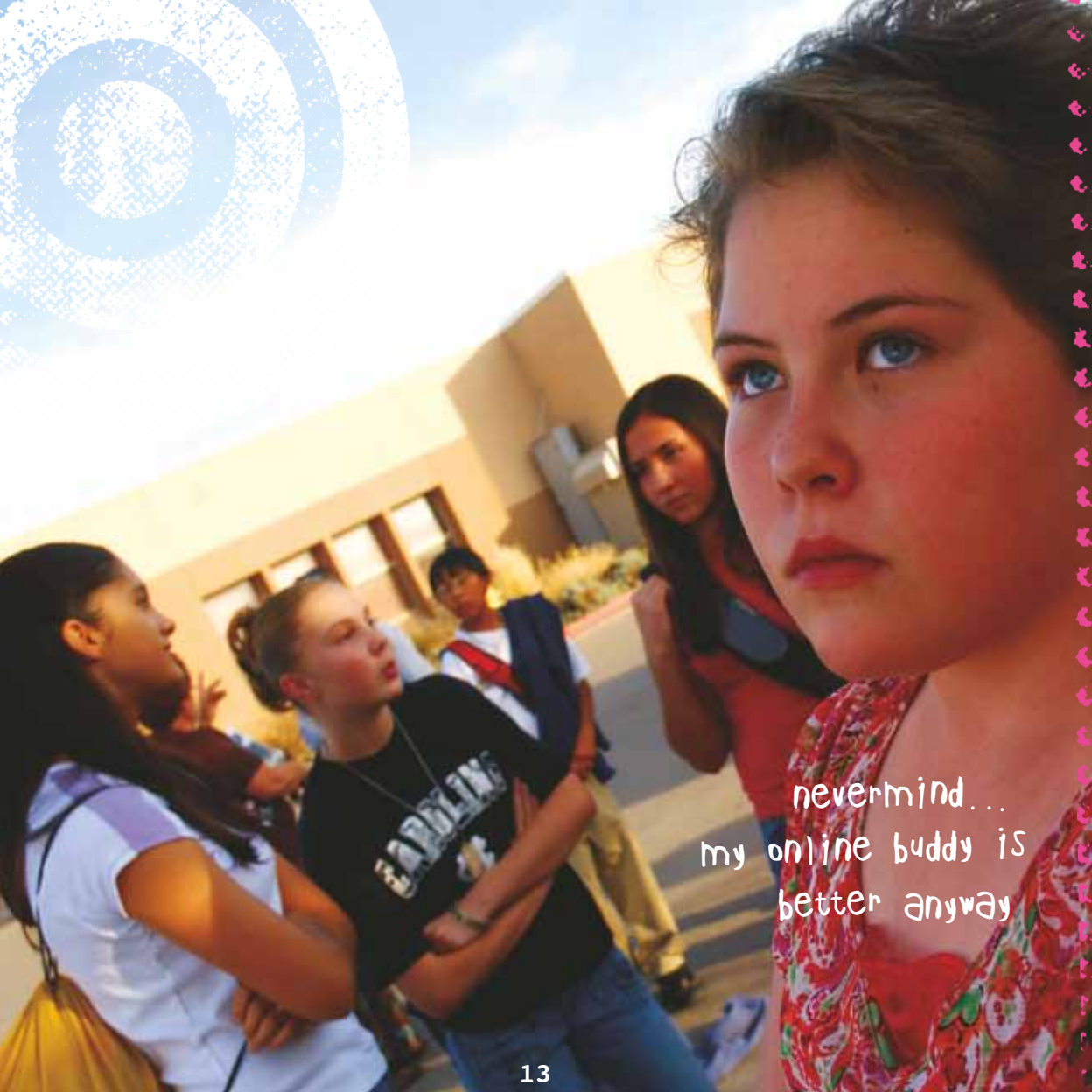
If it's adult porn, talk to your child. If it's child pornography, save the images but do not print or e-mail them, and contact the authorities immediately.

5. Your phone bill has calls to unknown numbers

There are a number of tools available online to search telephone numbers. Do a reverse phone directory search online to find out whose number it is. The reverse number search will give you a name and an address that is associated with the telephone number.



oh nothin just doin
research on the internet
for my paper



nevermind...
my online buddy is
better anyway

WHAT CAN YOU DO TO KEEP YOUR CHILDREN SAFE IN CYBERSPACE?

6. Your child receives mail/gifts/packages from senders you don't know
Track the package, research who it is from. Use the same tools the abusers use to find out information about them, such as reverse address directory searches, telephone directory searches, email address searches, Google searches, etc. Once the relationship reaches this level, it's time to intervene. A face-to-face meeting may be in the planning stages.

To report an unsafe situation online, go to websites like:
dcf.vermont.gov/stepup
www.sec.state.vt.us/otherprg/safeathome/safeathome.html
www.vtinternetcrimes.org
www.missingkids.org

If you suspect a face-to-face meeting has been arranged, contact local law enforcement immediately.

First and foremost, talk to your children openly and frankly. Be available to answer questions and concerns. Let them know about Internet dangers including identity theft, exposure to sexually explicit or violent material, and sexual predators.

Make it safe for them to come to you with concerns about people they've met online, when an inappropriate pop up appears or someone sends inappropriate materials to them and if someone harasses or threatens them online.

Educate yourself and your children about the risks involved in Internet use. People can pretend to be anyone, and their intentions are oftentimes not good.

Use separate user profiles, content filtering software and/or ISP filters, web browser controls, and/or your web browser's Internet history to monitor and filter what your child is doing on the Internet. Take the router out. See the section Tools for more information.



ONLINE ACTIVITIES and their POTENTIAL CONSEQUENCES:

1. Filling out online profiles

Filling out profiles will allow abusers and bullies to see personal information about your child, such as their real name, phone number, address, school name, etc. and will allow the abuser to “find” your child.

2. 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 where you or your child goes on the Internet, as well as key stroke trackers that may be used to steal your child’s identity.

3. Responding to postings that are belligerent or harassing

These messages are often posted by the author simply to get a reaction from people to see who will respond and to get a conversation going.

4. Posting pictures on the Internet

In addition to allowing anyone to get a look at your child, digital photo manipulation could put your child’s face on another body, which could be spread all over the Internet, or your child could be black-mailed into sending more photos.

5. Posting on blogs and social networking sites

Because these popular online features are virtual diaries, they give anyone online a more intimate look into your child’s thoughts and feelings. By reading postings on a blog, a bully or abuser can get a greater insight into a child’s vulnerabilities, likes and dislikes and can “tailor” a message targeted to your child. Even though it may take longer to learn about your child, the posting of your child’s thoughts and feelings may provide more information than even an online profile.

6. Chatting with strangers in a chat room

It's easy to lie online because a person's identity can be easily disguised, so seemingly innocent conversations can easily have harmful ulterior motives. Don't believe everything someone tells you in a chat room.

7. Using a webcam

For anyone who wished to harm your child, a webcam is the next best thing to an in-person meeting. By allowing people to view a webcam, your child is essentially opening the shades to your home or his/her bedroom and allowing a complete stranger to watch through that window. Anyone can use what they see to take advantage of your child. They may record the video your child sends and post it for the world to see or simply wait and use it against your child later.

8. Accepting webcam views from strangers

By accepting an invitation to view live webcams from strangers, your child could be exposed to nudity and sexually explicit material which could be disturbing. Ask your child to never accept an invitation to view a webcam or click on a link in a chat room.

9. Arranging a face-to-face meeting with someone met online

Your child could be hurt, molested, raped, kidnapped or worse during a face-to-face encounter.



Hi, ASL?

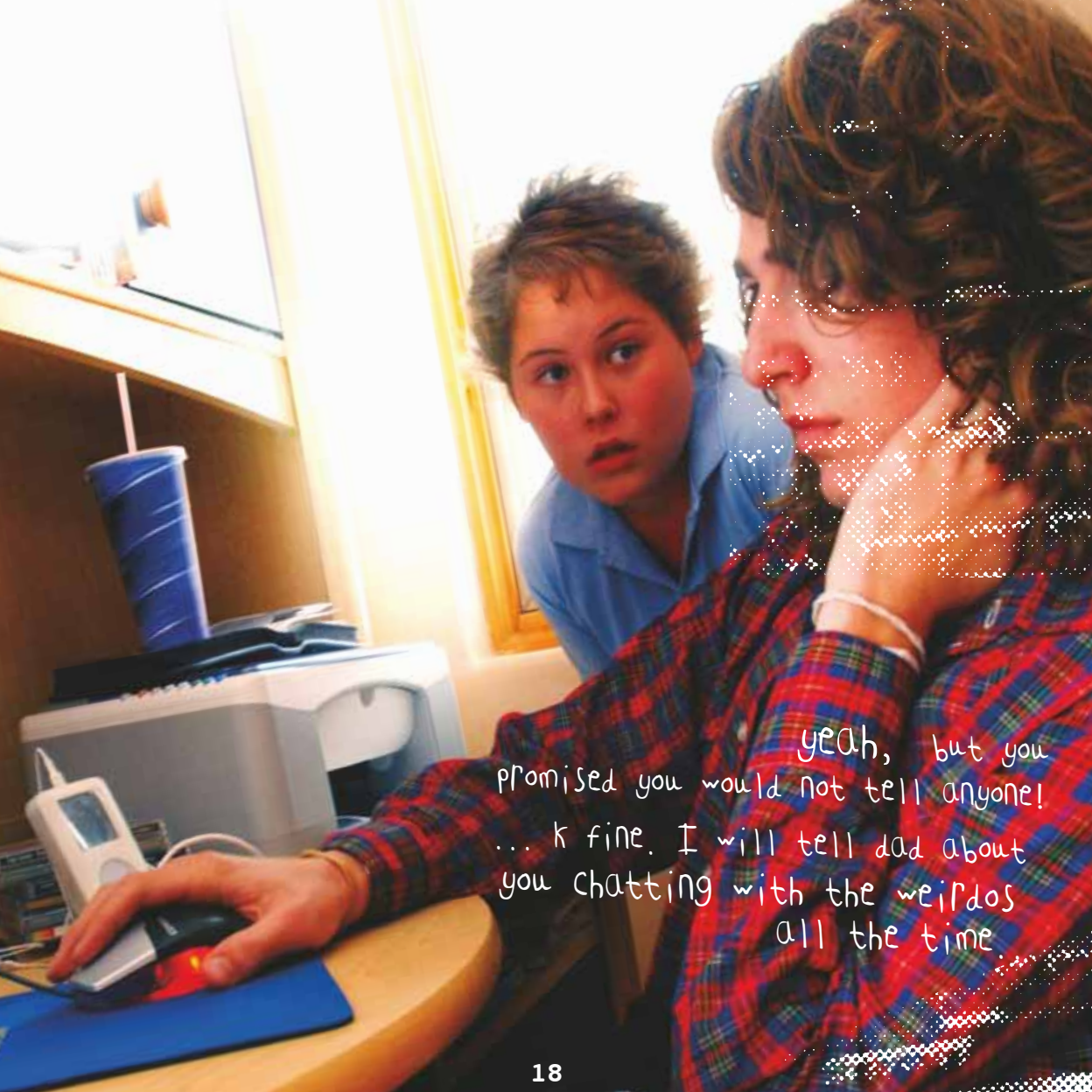


AGE APPROPRIATE GUIDELINES


Know the age rules for different sites. Then set your own standards. The rules and guidelines that you establish for young kids, preteens and teens will most likely be tailored to their ages and abilities. When establishing rules and guidelines, it's important to remember that teenagers are especially protective of their privacy, are the least willing to share what they are doing online, and will be the first to tell you that they don't want to be treated like a child. They are more independent online, more computer savvy and more likely to spend time in chat rooms and instant messaging than other age groups. Keep this in mind when you create age appropriate Internet usage rules for your kids. Also keep in mind that it is your responsibility to keep your children safe.

Here are some general guidelines to impress upon your kids, although some of them apply more to teenagers.

- BE EXTREMELY SKEPTICAL ABOUT BELIEVING WHAT YOU READ ON THE INTERNET, ESPECIALLY FROM SOMEONE IN A CHAT ROOM. It is extremely easy to lie online, especially if someone is trying to gain your trust so you will let your guard down.
- BE CAREFUL ABOUT WHAT INFORMATION YOU GIVE SOMEONE ONLINE, ESPECIALLY PERSONAL INFORMATION THAT CAN BE USED TO FIND YOU.
- DO NOT MEET SOMEONE IN PERSON THAT YOU MET ONLINE. Once your teenager has gotten their driver's license or if they use public transportation, it can be very difficult for you to prevent this from happening. You might want to express how dangerous it is to meet someone ALONE and if they cannot be persuaded to not meet someone from the Internet, to at least bring a friend and meet in a public place.
- DO NOT DOWNLOAD FILES A STRANGER HAS SENT YOU. They can contain inappropriate material or computer viruses.
- DO NOT VIEW THE WEBCAM OF A STRANGER.
- BE VERY SENSITIVE TO WHAT KIND OF INFORMATION YOU PUT IN YOUR ONLINE PROFILE, BLOG, OR SOCIAL NETWORK (i.e. MySpace or Facebook). Don't include any information that could be used to locate you. Remember to make your blog entries private or for friends only.



yeah, but you
promised you would not tell anyone!
... k fine. I will tell dad about
you chatting with the weirdos
all the time.



HONEY°
I JUST WANT YOU TO BE SAFE.

.. all right mom... i understand

How to talk to your teenager about Internet safety:

- Your teenager is gaining independence and struggling to get away from parental control. Protect them without alienating them by letting them have some independence while still providing parental guidance. Be involved with what they are doing on the Internet with appropriate respect for their privacy. Make sure they still feel comfortable talking to you about what they do on the Net.
- Teach your children to be critical thinkers. Show your teens that you trust them to make good decisions. Encourage them to protect themselves by being vigilant and cautious. Ask critical questions concerning the speed, intimacy or disclosures that an online friend pursues.
- Set reasonable expectations. You can't expect a teenager to completely avoid chat rooms, but you can expect them to not give a stranger their personal information.
- Remember, the Internet plays a critical role in their world. If you find they are doing something online you find inappropriate, choose a punishment carefully and remember that teenagers are going through a difficult and exciting time of change and new discoveries.

• Be supportive!

• Visit sites with your children. Clearly define for them what you consider inappropriate. Ask your child to show you how to navigate through the sites they have chosen. Google your child's name and explore privacy settings.



Learn about the Internet.

Don't put your head in the sand. Study. Some helpful sites for parents are:

www.netsmarz.org and www.getnetwise.org.

Get and install filtering software onto your computers. These websites can direct you to the right software that's best for you: www.getnetwise.org/tools/ or www.filterreview.com.

If you think your child might be engaged in suspicious activity on the Internet:

You can check the computer's Internet History to see the websites that have recently been visited. You can also take the computer into a computer services store. They can provide a full diagnostic evaluation to tell you exactly where your computer has been online and the types of activities that have taken place online using your computer.

WHAT TO DO IF YOUR CHILD BECOMES A VICTIM

If your underage child has received a SEXUAL SOLICITATION ONLINE, contact local law enforcement officials, the Vermont Internet Crimes against Children Task Force (www.vtinternetcrimes.org) or the National Center for Missing and Exploited Children (www.missingkids.com).

If you or your child has received CHILD PORNOGRAPHY, call local law enforcement immediately and do not delete the images. **DO NOT EMAIL or PRINT THE PHOTOGRAPHS!** If you do, you will be committing a crime.

If you have concerns regarding your child and their safety online, contact your local sexual assault support center at 1-800-649-5285.

INTERNET SAFETY TOOLS FOR PARENTS

A number of different tools can help you protect your children from the dangers of the Internet. Although none of them are foolproof, they can help. Here are a few:

- Be Accessible and Approachable
- Computer Placement
- User Profiles
- Web Browser Controls
- Viewing Internet History
- Filtering/Blocking/Monitoring Software
- Filtered ISPs

Be Accessible and Approachable

Monitoring online behavior may seem intrusive and insulting to your teen. Strong reactions, even concern, may seem judgmental. Show objectivity: step back, analyze, consider consequences. Model critical thinking. Consider personal boundaries. Show that you value their ability to detect and defend against online exploitation by developing their own critical thinking skills. Start this conversation when your children are still young.

Computer Placement

Remember, the family computer is not the only line of access to the Internet available to your children. They may also have easy access to Smartphones, school and community computers and other electronic devices. By keeping the computer in a common area of your home, you reinforce the message that Internet use must be responsible use and that there are consequences for inappropriate use.

User Profiles

Newer versions of Windows and Apple's OS allow for multiple user profiles to be set up. Every person who uses the computer can have their own user name and password. In order to gain access to the computer, the user name and password are required. This allows for different levels of access to be setup for each of the different users and also makes it easier to track and find out what each of the different users are doing on the computer. 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 inappropriate websites from being accessed. Web browser settings can be used in conjunction with user profiles to fine tune the level of access different users have on the Internet. By fine tuning these controls, you can customize the types of content that each user can gain access to. To get more information on using these settings, consult your browser's help files.

Viewing Internet History / Temporary Internet Files

In order 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. More savvy computer users can easily delete this information from easy access, but this information is still typically accessible by a computer expert. For more information about viewing Internet history and temporary Internet files, consult your browser's help files.

Software

Many different software programs available for purchase can help make the Internet safer for your children. Some of the options these programs can give you are:

- Blocking chat rooms and/or instant messaging
- 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 child-safe search engines
- Recording instant message conversations or chat room conversations
- Notifying you when your child tries to access an inappropriate website
- Limiting the time your child spends online
- Operating in the background without your child's knowledge
- Allowing third-party rating of websites



- Recording every key stroke your child makes
- Recording and sending you pictures of your child's computer screen as they are using it

Not all of these options are included in each software program. Each program is different. Compare some of these programs and find which one suits your needs.

Filtered ISPs

Most Internet Service Providers, such as AOL, Comcast, MSN and Time Warner may also be able to provide you with some filtering and blocking tools to help protect your child online. Contact them for more information.



OTHER IMPORTANT INFORMATION to protect you and your family online

You are responsible for what you post on the Internet. To avoid unsafe situations for you, your family or for others, **THINK BEFORE YOU ACT**. Understand what it means to be a critical consumer of the Internet.

IF SOMETHING SEEMS TOO GOOD

TO BE TRUE, it probably is. Don't believe someone wants to give you money for nothing.

FORWARDING A MESSAGE MAY PERPETUATE

A MYTH. Don't help spread another "Urban Legend" around the Internet. Learn the truth at websites like www.snopes.com or do an Internet search. Spreading rumors is wrong offline and it can be even more harmful online because it can spread faster.

SUCCESSFUL FRAUDS AND SCAMS

LOOK LEGITIMATE. Don't let an authentic-looking email that appears to be from your bank, credit card company, lottery commission, or representative of a will or estate fool you into revealing your personal information or sending money.

Tristram J. Coffin
United States Attorney
District of Vermont



CHECK IF THE SITE IS SECURE.

Remember, while more secure sites have a small padlock icon in the lower corner of your browser and the address starts with "https" rather than "http," this does not guarantee that the site is legitimate.

EMAILS that ask you to respond (or your account will be closed) are typically an attempt to steal your personal financial information.

"UNSUBSCRIBING" TO UNSOLICITED MESSAGES only confirms to spammers that you're receiving their emails.

OPENING AN ATTACHMENT FROM AN UNKNOWN SENDER, especially ".zip" files, may install viruses that can damage your computer and possibly the computers of everyone in your address book.

INSTALL UPDATED VIRUS AND SPYWARE PROTECTION to prevent your computer from becoming infected.

INSTALL A PERSONAL FIREWALL ON YOUR COMPUTER to prevent hackers from secretly installing spyware or accessing files on your computer.



**KEEP ON TOP OF
THE LATEST SCAMS**

You can access consumer alerts at the Attorney General's website: www.atg.state.vt.us and click on Consumer Protection



Tristram J. Coffin
United States Attorney
District of Vermont

LMIRL

for teens
internet safety guide

Dear Vermonter,

I am sure that I can't tell you anything new about the Internet. You've probably used computers since you were old enough to reach a keyboard. I am also sure that you know quite a bit about being smart and safe on the Internet. As you know, there are risks associated with Internet usage. Others use the Internet to victimize people your age. I hope you will take some time to read this booklet, which will confirm two important safety points: First, it is easy to deceive online; second, when you post online, nothing is private, ever. Anyone can share everything you give them with anyone anywhere in the world.

Online danger comes from many places. You may find yourself in an unsafe situation when strangers ask to add you as a friend or when you have accidentally given out too much private information, such as your address or photographs. Sometimes, the danger comes from harassment between people you go to school with, hang out with or live near. Sometimes, it may be directed at you. Sometimes, you may be causing it without knowing you are. Any of these situations can spin out of control.

With these possible situations in mind, here are some things to remember: Don't react. People who harass others feel powerful online. They just want to get a reaction - any reaction. Don't join in. Instead of contributing to rumors, ask yourself, how you would feel if these were rumors about you? Sending hurtful or untrue information to others is just as bad as starting a rumor yourself. Stand up to unkind behavior. By showing the courage to speak up, you take some of the abuser's power away. Say something supportive to the target or tell an adult you trust. Do not engage in conversation with someone if you suspect they are dangerous. Save the evidence. Save upsetting information and bring it to someone you trust. And never, ever post or send information or photos that you do not want your family, your friends or anybody else to see. The most important thing is to stay smart. Ask questions. Is this relationship appropriate? Would I disclose this information to another person if it wasn't on the Internet? Where can I search to prove the accuracy of this statement? Would I want my teacher or future employer to see this photograph on the Internet? How do I get out of this situation if necessary? Remember, stay alert and stay in touch with people you trust. The Internet is a powerful tool that brings the world to your desktop. We all just want to make sure you use it safely and responsibly.

Thank you,

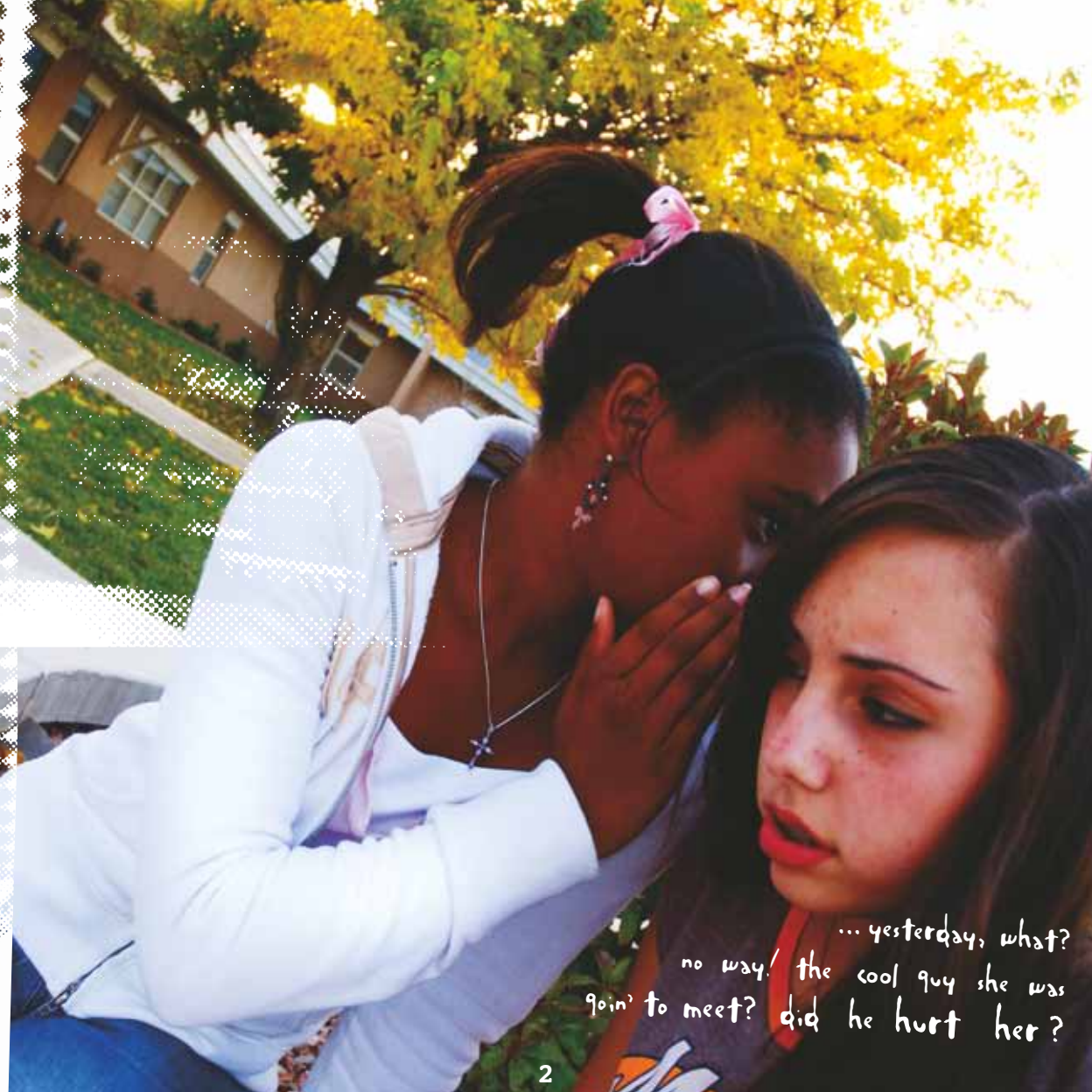


Tristram J. Coffin
United States Attorney
District of Vermont





victor how about tomorrow
victor are you home alone again
socccgrl yeah
victor lets chat tomorrow
at the same time then...



... yesterday, what?
no way! the cool guy she was
goin' to meet? did he hurt her?

WHAT'S THE PROBLEM?

The Internet can be a really great tool, fun to surf in your spare time, and totally entertaining. But remember, some things are just too good to be true.

Unfortunately, we live in a world where people sometimes take advantage of others. It's good to be prepared; this may happen to a friend or a sibling or to you. Anything on the Internet, whether it's chat rooms or web sites, that attracts you and your friends will also attract abusers, bullies and predators.

>>> Read on.

Many predators, people searching for young adults and teens to rape, kidnap or harm, now use the Internet as their tool of choice. Instead of doing research, like you are doing for that English paper, a predator uses the Internet to find victims. Predators communicate through chat rooms and instant messaging seeking to develop relationships with young people. They seek the trust of young people. When a trust forms, they ask to meet somewhere to check out a movie, window shop or

get something to eat. Typically, a predator does all this while posing as a young adult or teenager himself.

Who are the cyber predators?
Not who you think:

- >> Most are male
- >> Above average intelligence
- >> Above average incomes
- >> Have a successful career
- >> Most are white
- >> Have computer knowledge
- >> Many have children of their own
- >> Have no criminal history related to sex crimes
- >> Most are older than 26

HOW THEY LURE YOUNG PEOPLE:

Predators use the anonymity of the Internet to talk to young adults. They look for clues to figure out what you like, who you are and sometimes, even where you live. Too often, it's made easy because information has been volunteered by young people.

1/ USER NAMES / SCREEN NAMES:

While a user name or screen name seems like a pretty innocent thing, it can be a gold mine of information for the viewers. You might think about your favorite bands, pets, hobbies and sports as part of a user name or screen name. But by doing so, what information have you given someone who may want to hurt you to use?

User name:

Abercromshoper89.

This tells the viewer that you like to shop, Abercrombie and Fitch is a favorite of yours, and that you were born in 1989.



User name:

Prisonerofhermione15.

This tells the viewer that you are a Harry Potter fan, you especially like the character Hermione Granger, and you are likely 15.

Armed with this information, a person with bad intentions will talk to Abercromshoper89 about shopping and fashion while talking to prisonerofhermione15 about Harry Potter and magic.

It may not seem important, but providing this information helps a potential abuser learn how to become a trusted friend and is unnecessary and potentially dangerous.

WHEN CHOOSING A USER NAME OR SCREEN NAME, think of the game "MadLibs." Try using one of the following formulas to select a user name:

>>> Adjective + noun

stuffedninja

>>> Size + animal

minielephant

>>> Season + noun

summerteeth

>>> RANDOM number + ice cream flavor

45cookiedough

>>> Actor's name + action verb

Travoltadancing

>>> Color + foreign food

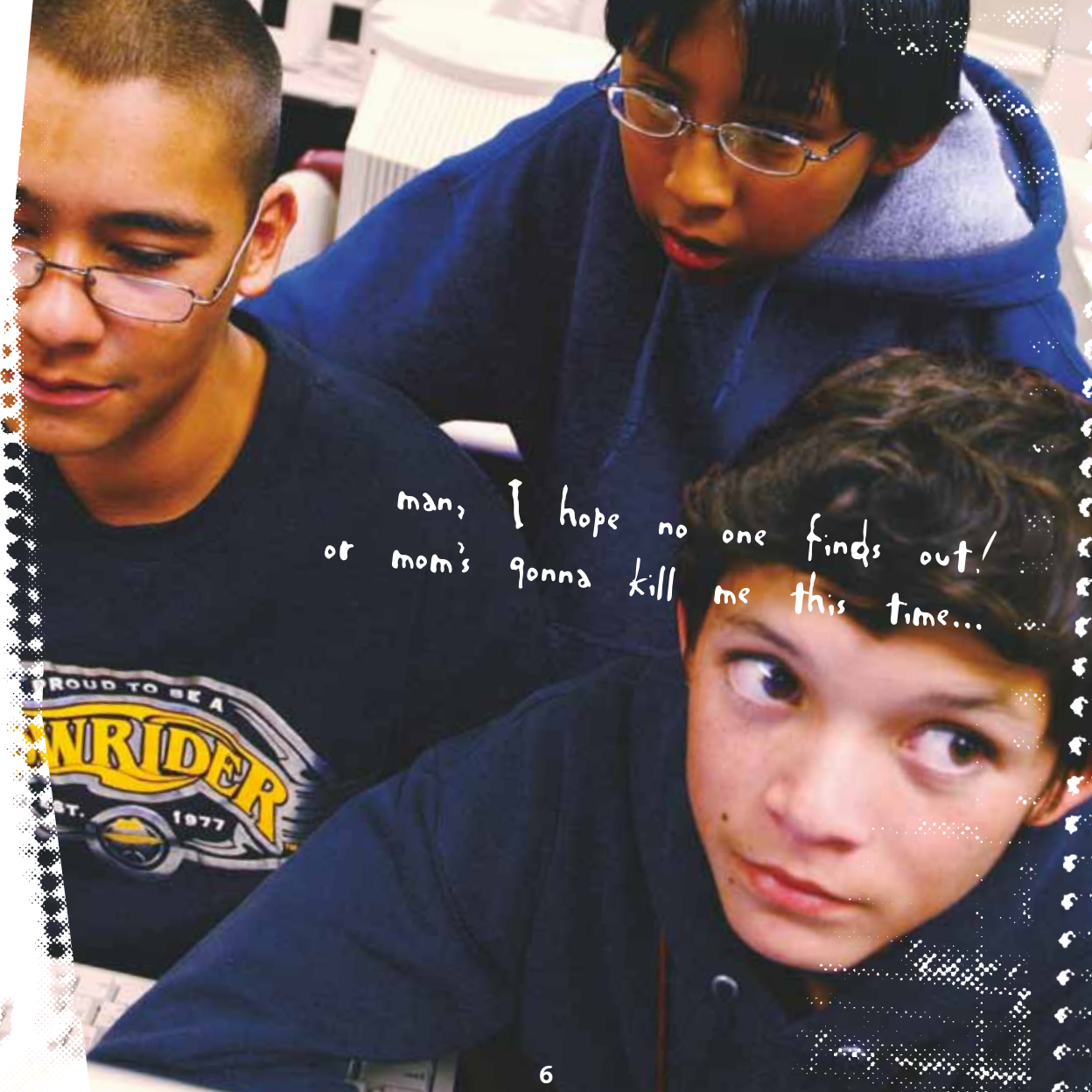
pucebaklava

A user name or screen name with a random selection of words such as "Soupshoe" is much better than a potentially descriptive identifier such as "Missy1981". Make sure your user identifier doesn't relate to you, your age, your school, your location, or your interests.

and have fun with it!

A close-up, profile view of a woman with dark hair looking intently at a computer monitor. The scene is dimly lit, with a warm yellow glow from the computer tower and keyboard area. A large, semi-transparent target graphic with concentric circles is overlaid on the bottom right corner of the image. The text is positioned on the left side, over the dark area of the screen.

**see finally someone
who isn't just pushing me around**

A photograph of three young men in a classroom setting. One man on the left is wearing a black t-shirt with a 'HARLEY-DAVIDSON' logo. A man in the middle is wearing glasses and a blue hoodie. A man on the right is looking towards the camera with a wide-eyed expression. The image has a halftone dot pattern on the right side.

man, I hope no one finds out!
or mom's gonna kill me this time...

2/ PROFILES:

Profiles can provide abusers and bullies with a lot of useful information. Profiles ask for information like your real name, birthday, address, phone number, hobbies and what school you go to. Filling out this information is meant to be useful to other teens and young adults who are looking for people to chat with who are interested in the same things.

The problem is that those who want to manipulate you use personal information to gain your trust. Filling out profiles is not required to use most chat programs. To protect yourself, fill out profiles only on sites that allow you to control who has access to the profile.

3/ WHAT YOU SAY:

Some abusers will do something called "cyberstalking" (and yes, it's as scary as it sounds). An abuser will go to a teen or young adult chat room and pick a user name to follow through chat rooms. The abuser will slowly accumulate information about that user by simply reading what they are chatting about with other chatters. Young adults and

teens face many problems with peer pressure, parents, friends and other family members. Chat rooms seem like the perfect place to gripe about all those people who are disturbing your life, but watch out for people too anxious to relate. Often, abusers will play on your emotions by saying they went through the same thing.

4/ SELLING STUFF:

By selling things online, you can always make a quick buck off of things that you no longer use. But selling things can also provide dangerous information. Sometimes, a seller will provide their telephone number so that people interested in purchasing can call and ask questions about the item. Predators will use your telephone number to track you down. Providing your phone number not only identifies the state you live in, it also can lead to your doorstep.

THEIR TECHNIQUES:

Identifying a cyber predator is difficult because they sound like anyone else. Chatting online can be really fun and can be a quick way to make new friends, but it might not be the safest way. Predators, bullies and harassers have many techniques that they use to convince you that they are just like you, can relate to your problems, and would like to become your real friend instead of your online buddy.

Giving you special stuff:

Sometimes there are things that you may or may not want to see, like Playboy pinups or other sexually explicit material. Sometimes curiosity gets the best of us, but safety is always the most important thing to remember. When an online buddy sends you sexually explicit material,

whether you want it or not, it is smart to stop speaking to that buddy. Predators use this technique to scare or befriend you. Almost all of the time this material is unwanted, but if you continue to speak to this person, they will push you to do more things than just look at inappropriate material. Ending the conversation will tell that person that you are not interested in what they have to offer as an online buddy any longer.

Pretending:

We've mentioned that abusers will often disguise themselves as teenagers and young adults. Sometimes they will let you know that they are adults, but most often they will befriend you online as a peer. These people can be very convincing and, without realizing what you have done, you may befriend someone who wants to

hurt you. There really is no way to know who is your same age and who is an adult, but being safe means ending communication with any online buddy who begins to harass you. Remember, never give out too much personal information (not even an email address) and if anything mean or inappropriate happens, don't be afraid to tell your parents or someone you trust.

Threats:

If an online buddy begins to threaten you because you refuse to meet him or speak to him anymore, the best thing to do is tell your parents or a trusted adult. Bullies exploit any weaknesses they can find. Their objective is to make you do what they want, whether or not you want it. Getting advice from an informed adult will help you make the right decision and will make sure you stay safe.



wow, thats pretty nasty...
scroll down now

...tony is cute i guess, but the guy ive met on the internet last week is sooo much cooler
he is 18 he said and i think he likes me 2... and then he sent an email and said i look totally
hot in that picture... he said he wants to meet...



LOVE IT

User name tracking:

Searching chat rooms or reading your blogs (online journals) are easy ways for anyone to learn how to talk to you and earn your trust. By following you through chat rooms, an abuser can gather information about you and make you feel comfortable enough to talk to them about anything, even revealing secrets. Beware of someone who knows everything about conversations you have been having or is quick to say "the same thing happened to me."

Photographs:

Putting photographs online is becoming more and more popular, especially with chat rooms, blogs, and online social networks like "facebook.com." Unfortunately, there are a number of reasons why photographs are a problem:

- Combining a photograph with personal information can make it extremely easy for a dangerous person to find his way to your school or doorstep.
- Photographs can be manipulated—your face put onto another person's body in a sexually explicit photograph—and posted for anyone, including your parents, to see.
- Pictures may be fun, but make sure that you only post pictures in places where only people you know can view them.

Be very careful when putting your photo online.

Email:

Sometimes you meet people who you really like online and you want to talk to them more than just in chat rooms. Giving out your email address or instant messaging screen name can be a good way to keep your conversation private. But be careful when you give out your email address. Your email address is personal, and it is unsafe to give it to online buddies because they can use it to discover more information about you. Limit the people who have your email address to friends and family; try not to give it to people you meet in chat rooms, and set your chat profile so that it does not display your email address.

- It is important to understand that a predator wants a picture of his prey. He will ask for a photo. He may ask for you to pose partially or completely undressed. If you send a picture of yourself that you would not want your parents or friends to see, it can be used to blackmail you into sending more. A predator is trying to control the person he is preying on. **This is not a relationship about love; it is about control.**



THE GROOMING PROCESS.

Predators groom their victims. The objective of grooming is to manipulate the victim into behaving in whatever manner the predator wants.




- 1 Charlie starts chat, expresses feelings that the predator can easily pick up on.
- 2 Predator begins “grooming” by expressing empathy to gain Charlie’s trust.
- 3 Charlie further expresses trust in the person he/she is chatting with, encouraging the predator.
- 4 Predator continues to sympathize.
- 5 Charlie’s frustration is evident to the predator who takes full advantage of Charlie by portraying himself as a trusted confidant.
- 6 Predator offers a way to entice Charlie.



- 1 Charlie89: my mom sux!
its her falt that my parents are gettin divorced
- 2 PREDATOR: i no.
my parents r2.
C: we never have \$\$ nemor
- 3 C: evry time i need somethin she says the same thing “we cant aford it”
C: when my parents were 2gether i could buy stuff
C: now i cant
- 4 P: me to. i hate dat.
C: i w8ed 6 mos for this game to come out
C: my mom promisd me wed get it.
C: can i get it now? nope.
C: we dont have enuf \$\$\$.
my mom sux!
- 5 P: wow. thats tuf
P: i hav a realy cool uncle
P: buys me things all the time
P: he has lots o \$\$\$

- C: ur sooooo lucky!
- 6 P: i got an idea. ill see if hell by it 4 u.
- C: really? thx man!
- 7 P: brb gonna call him
- 8 P: w00t! he said k
- C: wow realy? thx i cant bleve it.
- 9 P: where do u live?
- C: brlngtn, vt u?
- 10 P: plattsburgh, ny unclie 2. ne malls near u?
- 11 C: university mall.
- P: ive herd of that one. Saturday ok?
- C: sounds good.
- 12 P: b ther at 12
- C: k. meet at the game store.
- P: k!
- C: well g2g. thx again dude
- C: this is awesome!
- C: TTYL!
- P: l8r



- 7  Of course, there is no “rich uncle.” The predator gives that impression to Charlie by waiting for a period of time before sending his next message.
- 8 Predator expresses excitement, tells Charlie the “uncle” will buy the game.
- 9 Predator starts asking for clues about Charlie, begins the process of scheming to find out where Charlie is to arrange a face-to-face meeting.
- 10 The predator will place himself in close proximity to Charlie, regardless of his actual location.
- 11 Charlie has actually just determined the final meeting place without realizing the danger he/she is in, even though trust has been built up with the new “friend.”
- 12 Predator finalizes the meeting.



The predator now has all the information he needs to meet you face-to-face.

Here's an example of an online chat you could experience and how you might find yourself being “groomed” by a cyber predator:



WIBNI...



Soccrgrl29 is chatting with a potential predator. **WHO** is it?

Bob174: Hi

Soccrgrl29: Hi

Bob174: ASL?

Soccrgrl29: 13/f/
usa.u?

Bob174: 14/m/usa

Soccrgrl29: mm.. guess not

Bob174: y r u not at school?

Soccrgrl29: day off. yay :)

Bob174: kewl. so ur home alone?

Soccrgrl29: ya.parents r at work

Bob174: do u have a bf?

Soccrgrl29: no

Bob174: do u want 1?

Soccrgrl29: yes... :)



LikeMikey22: Hi

Soccrgrl29: Hi

LikeMikey22: asl?

Soccrgrl29: 13/f/usa.u?

LikeMikey22: 14/m/usa. u like soccer?

Soccrgrl29: yea, it's my fave sport. i'm a forward

LikeMikey22: cool. me to :Jwhat else do u like to do

Soccrgrl29: hang out with my friends, go shopping at the mall, go to the movies. u?

LikeMikey22: skateboard, hang out, play hackeysack, watch tv

Soccrgrl29: cool. skateboarding looks

like fun but i bet i would fall


LikeMikey22: it's not that hard

Soccrgrl29: maybe i'll try it someday :)




maybe i'll try it someday...

The answer: Both Bob174 and LikeMikey22 could be potential predators. But the most recognizable predator is Bob174. He asks highly personal questions and wants to know if Soccrgrl29 is alone.



1 in 7 young people
have received unwanted
sexual solicitations online ←

1 in 3 young people
have been exposed to
sexually explicit
pictures online without seeking
or expecting them ←



1 in 17 young people have
been threatened ←
or harassed online

1 in 25 young people have
received an aggressive
solicitation
→ to meet
somewhere




yeah, he said
he would get me into the
concert tomorrow FOR FREE!

he knows the drummer
really well!
Yeah, he's cool...

EXIT

WELL YEAH, BUT HE IS
SO NOT THE GUY
I THOUGHT ... AND HE
IS LIKE ... STALKING ME NOW!
... DON'T KNOW
HE IS SCARING ME ...
NOPE, BUT DON'T
TELL ANYONE





Whether online or offline, almost everything you do has a consequence. If you do it online, it, and the consequences, may be memorialized forever. Always ask yourself what the possible long term consequences could be—no matter how far-fetched. Remember, anything you post on the Internet may one day be seen by the admissions officer from your favorite college, a future employer or even a future boyfriend or girlfriend.

1. Posting pictures of yourself on the Internet

In addition to allowing anyone to get a look at you, digital photo manipulation can put your face on another body, in any graphic or degrading situation. When such an embarrassing photo is in the possession of an abuser, it can have devastating consequences. The abuser might threaten to send the picture to your parents or spread it all over the Internet unless you do as he says.

2. Posting on blogs and social networking sites

These features are virtual diaries that give viewers a more intimate look into your thoughts, feelings and vulnerabilities. This information could be exploited by cruel or dangerous individuals. Be aware of facts you post that identify your school, community or family.

3. Responding to postings that are belligerent or harassing

These messages are often posted by the author simply to get a reaction – any reaction. If you do respond, you may open yourself to harassment. Don't join in. Instead of contributing to rumors, ask yourself how you would feel if you were the target. Forwarding hurtful or untrue information is just as bad as starting a rumor yourself. Stand up to unkind behavior by peers. By showing the courage to speak up, you take some of the abuser's power away. Say something supportive to the target or tell an adult you trust. Do not engage in conversation with someone if you suspect they are dangerous. Save the evidence. Save upsetting information and bring it to someone you trust.

4. Chatting with strangers in a chat room

Giving out information to people online is just as dangerous as giving the same information to a stranger you meet on the street, maybe even more dangerous.

5. Using a webcam

By allowing people to view your webcam, you are essentially opening the shades to your home or your bedroom and allowing anyone to watch you through that window. Predators and harassers will use what they see to take advantage of or harass you. Once images of you are online, they are online forever.

6. Accepting webcam views

By accepting an invitation to view live webcams, you could be exposed to unwanted nudity and sexually explicit video which could be disturbing. Remember, that 16-year-old that is inviting you to see him is more likely to be around 50, overweight and hairy.

7. Arranging a face-to-face meeting with someone you've met online


Since it is not possible to know who you are really talking to online, you may be unpleasantly surprised when you discover that person's true identity. It is very possible that the person has misled you with the intent to harass or hurt you, even to molest, rape, kidnap, or kill you.

8. 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 where you go on the Internet, as well as key stroke trackers that may be used to steal your identity.

9. Filling out online profiles

Filling out profiles will allow others to see personal information about you, such as your real name, phone number, address, school name, etc., and will allow the abusers to "find" you offline.



he sent me ugly pictures again -
I don't like him any more...
he said he's gonna tell my mom
what we chat about
if I don't call him back
though

CYBER SAFETY GUIDELINES:

Help catch abusers, bullies and harassers and protect your friends. Even if you are safe, someone you know may be the next target. Report any of the following to a local police officer.

>>> Threats, bullying, harassment
- save the communication by copying and pasting into a text file.

>>> Sexually explicit pictures or streaming video -
do not print it or send it. Save the information.

>>> Sexual solicitation -
save the communication by copying and pasting into a text file.

- Don't stay in an uncomfortable or dangerous situation online. You might hesitate to tell your parents because they may not approve of how you got into the situation. But you should realize that a bad situation could get worse if you ignore it.

Know your social networking privacy settings.

>>> You can limit access to your information, photographs and conversations. Only those you trust should be close to you online.

>>> When starting new friendships, always ask yourself: Is this friendship moving to intimate subjects too quickly? Is this too good to be true? Would I answer that question if someone asked me face to face? Do I want my future employer, boss or coach to see that picture?

- Share these guidelines with your friends and siblings.

You can get more information about online safety at:

www.netsmartz.org

www.atg.state.vt.us



**STEP UP:
PROTECT KIDS FROM SEXUAL ABUSE**

WEBSITE: [HTTP://DCF.VERMONT.GOV/STEPUP](http://DCF.VERMONT.GOV/STEPUP)

**CHILD ABUSE HOTLINE:
1-800-649-5285**

**CHILD SUPPORT HELPLINE:
1-800-786-3214**

what? really?
he said he's gonna copy the latest CD for you?
oh sweet, man. you are meeting him at the park?
Yo. Later.

which of these two people should dirt_rider_15

be **suspicious of ?**

mx_racer45: hey dirt rider

dirt_rider_15: hey

mx_racer45: ASL

dirt_rider_15: 15/m/ut

dirt_rider_15: u

mx_racer45: 17/m/nh

mx_racer45: darn hoping u would be girl

mx_racer45: but no problem, u ride moto thou?

dirt_rider_15: yeah 4 fun

mx_racer45: awesome me 2

mx_racer45: what u ride?

dirt_rider_15: kx250

dirt_rider_15: u?

mx_racer45: yz400

mx_racer45: u have pic of it?

dirt_rider_15: yeah, I send it.

dirt_rider_15: u have 1?

mx_racer45: great look n bike

dirt_rider_15: yours 2

mx_racer45: I liv in manchester, nh, where u liv?

dirt_rider_15: rutland, vt

mx_racer45: where that?

dirt_rider_15: near castleton

mx_racer45: cool

mx_racer45: maybe we can rid some time

dirt_rider_15: cool

The answer: Both mx_racer45 and moto-boy77 could be potential predators, but moto-boy77 is more suspect. He tries to set up a meeting and asks for pictures.

moto-boy77: Hey dirt rider
dirt_rider_15: Hey
moto-boy77: ASL
dirt_rider_15: 15/m
dirt_rider_15: u
moto-boy77: 17/m,
moto-boy77: 2 old for u?
dirt_rider_15: no
moto-boy77: I c u ride motocross
dirt_rider_15: just 4 fun
moto-boy77: cool
moto-boy77: I also ride 4 fun,
moto-boy77: I used to compete
dirt_rider_15: y u stop?
moto-boy77: 2 busy
moto-boy77: where do you live, maybe we can go
ride sometime?
dirt_rider_15: I am not supposed to say
moto-boy77: Ok but I thought it might be fun if
showed you some cool tricks
dirt_rider_15: I guess it would be ok
dirt_rider_15: rutland, vt
moto-boy77: Is that near burlington?
dirt_rider_15: kinda howd u know?
moto-boy77: I have friend in burlington that I
am going to visit in a few weeks
moto-boy77: do you want to go ridding then?
dirt_rider_15: that would be cool
moto-boy77: u have pic?
dirt_rider_15: yeah why?
moto-boy77: I like 2 no who I'm talking 2
dirt_rider_15: o, I'll send it
dirt_rider_15: u have 1?