HOW SAFE IS YOUR CHILD FROM CYBER-SHARKS?

PAULA D. SILSBY
United States Attorney
District of Maine

internet safety guide
for parents

even YOUR CHILD

can become a target

Dear Parent,

The Internet is now a vibrant part of our daily lives. We e-mail, shop, share photographs, and connect with friends and family — all online, and in our homes. Yet this amazing tool can also bring into our homes, and our children's lives, some of the worst dangers imaginable.

Online predators use the internet to approach young people for sexual favors, sexually explicit photographs and a wide variety of other inappropriate — and usually illegal — activities. Without knowing it, our children often make a predator's job easier by sharing personal information that leaves them vulnerable to online exploitation. Online predators are highly skilled at using this personal information to befriend children and victimize them.

Parents must be the first line of defense against online victimization of their children. It is in this spirit that we enclose our newest publication, "Internet Safety Guide". I urge you to read this booklet carefully and 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, and that effort will be most successful if all parents teach online safety at home, monitor their children's Internet activities, and talk openly with their children about the risks. Your children are much less likely to be victimized if you're actively involved in their Internet usage and help them understand the risks they face online.

I encourage you to explore the www.NetSmartz.org online resource guide on Internet safety and computers, and hope you find this booklet a helpful resource for beginning the discussion with your children.

Paula D. Silsby
United States Attorney
District of Maine

MECASA
MAINE COALITION
AGAINST SEXUAL ASSAULT

www.mecasa.org

STATEWIDE SEXUAL
ASSAULT CRISIS AND
SUPPORT LINE
1.800.871.7741
TTY 1.888.458.5599

Your local sexual assault support center is an excellent resource for you and/or your child if they have been a victim of an online predator.

This is a confidential 24-hour toll-free hotline accessible from anywhere in Maine. Calls are automatically routed to the closest sexual assault support center.

www.maine.gov/ag

VISIT THE CHILDREN & FAMILIES LINK AT THE MAINE ATTORNEY GENERAL'S WEBSITE

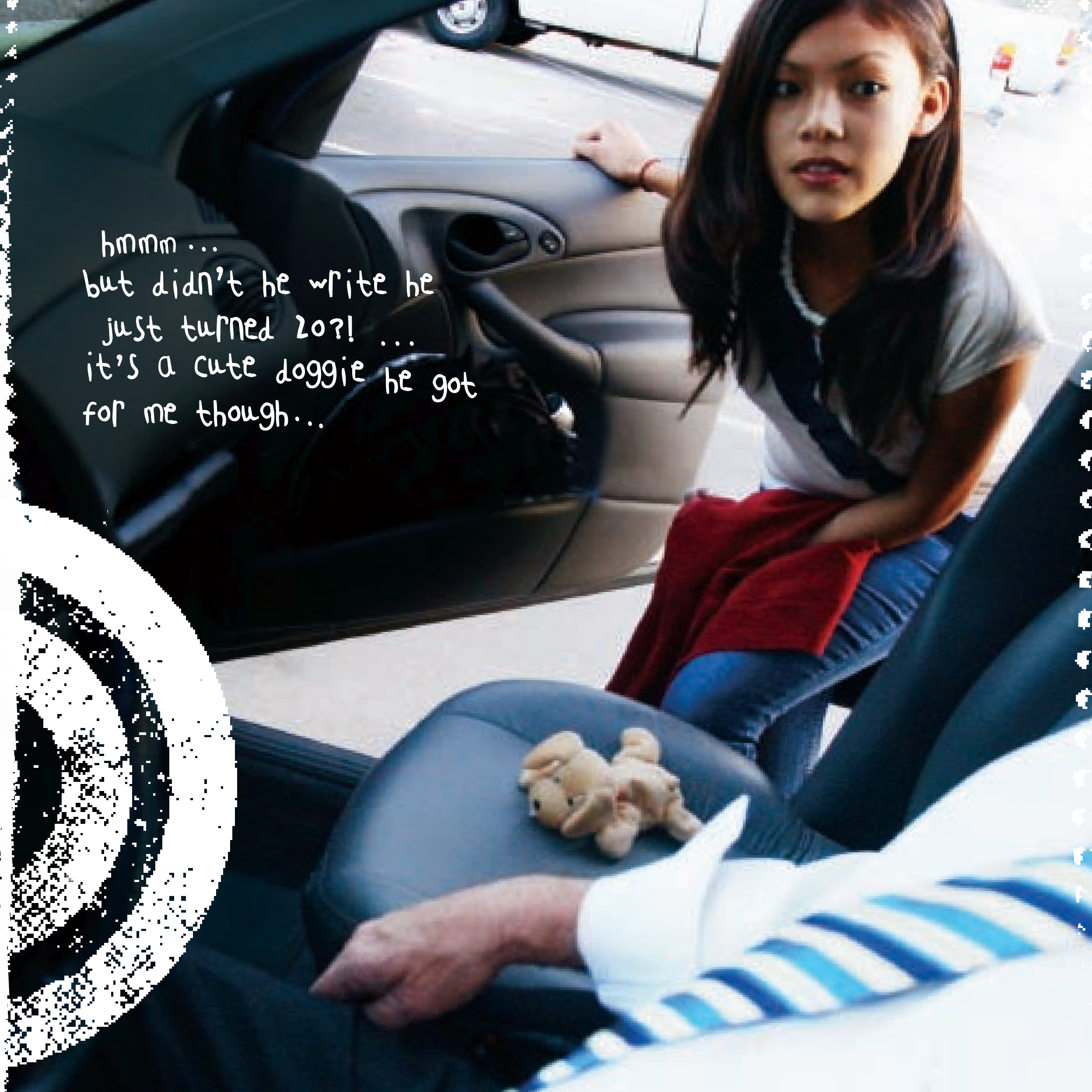
The Internet is a huge information source and it's a valuable tool for adults and children. But because of its anonymous nature, it is also a breeding ground for predators.

IN REAL LIFE, 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. The predator has direct access to your child.

If you would like an Internet Safety presentation in your community or school, you can contact the office of the Attorney General at 1-207-626-8800 or your local sexual assault support center at 1-800-871-7741.

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


hmmm...
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 have been sexually solicited online

>>> 1 in 3 youth have been exposed to sexually explicit pictures online without seeking or expecting them

>>> 1 in 10 youth have met someone face to face they met online

>>> 2 out of 5 youth trust the people they talk to on the Internet

>>> More then 80 percent of youth spend at least an hour a week 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 (99%), white (91%), and older than 26 (86%)**
- **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 youth is saying – within 45 minutes they can access 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.**

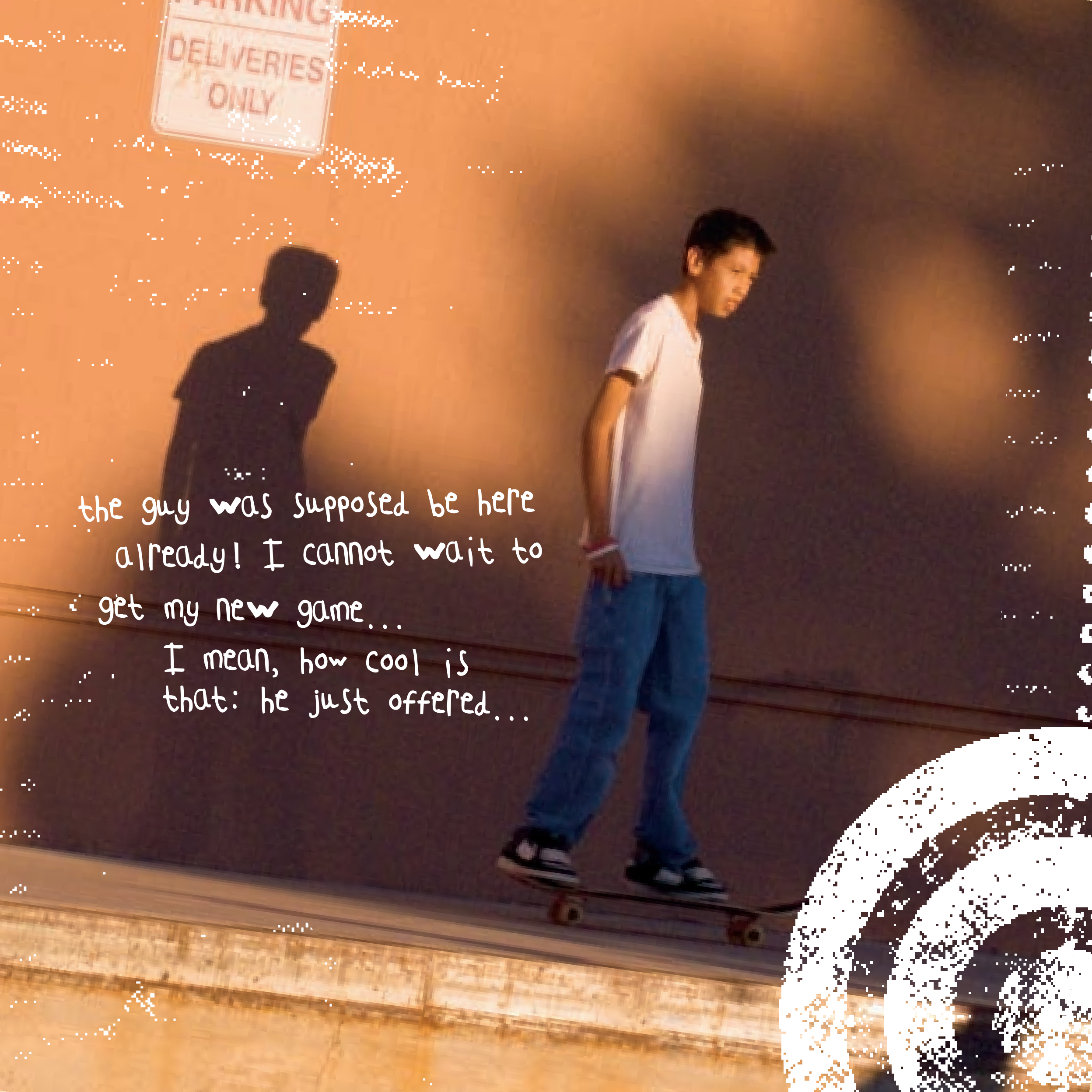
The predator can then ask to be included on the child's "buddy list" and be able to tell every time the child is online. A buddy list is a feature that keeps the names and addresses of others who are contacted frequently in a chat room, somewhat like a chat room address book. When a user signs into an 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.

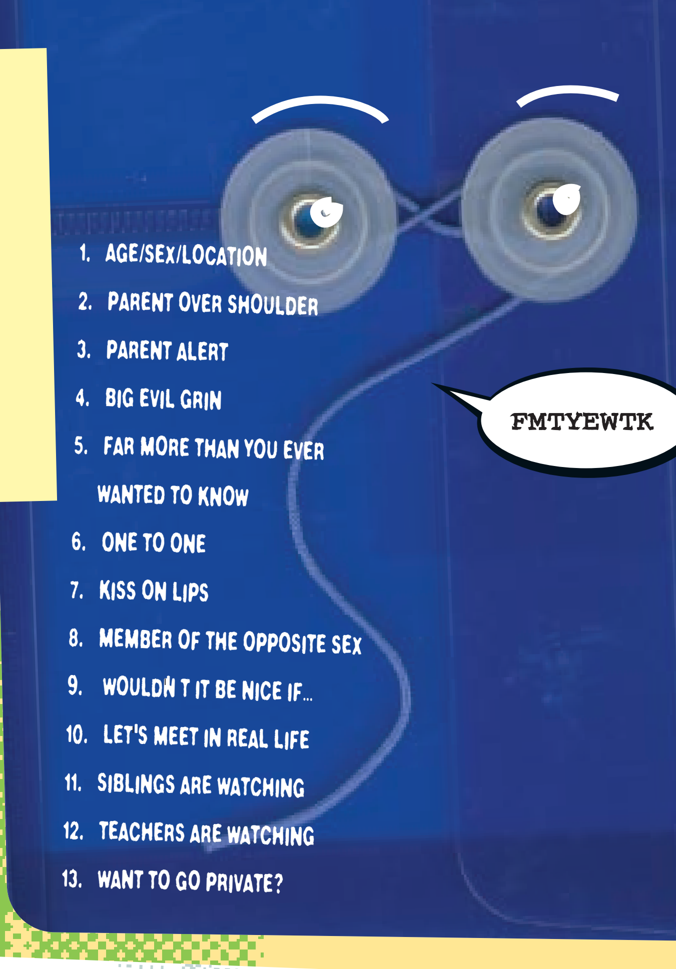


the guy was supposed be here
already! I cannot wait to
get my new game...
I mean, how cool is
that: he just offered...

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. WOULDN 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?

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 <u>EXAMPLE OF AN ONLINE CHAT</u> 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: ptlnd, me u? *("Portland, Maine. You?")*

PREDATOR: portsmouth, nh uncle 2. ne malls near u? *("Portsmouth, New* J *Hampshire. Uncle, too. Any malls near you?"* K

CHILD: maine mall.

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.

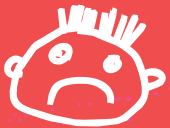
K Child has actually just determined the final meeting place without realizing the danger he/she is in, even though trust has been built up with the new "friend."

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

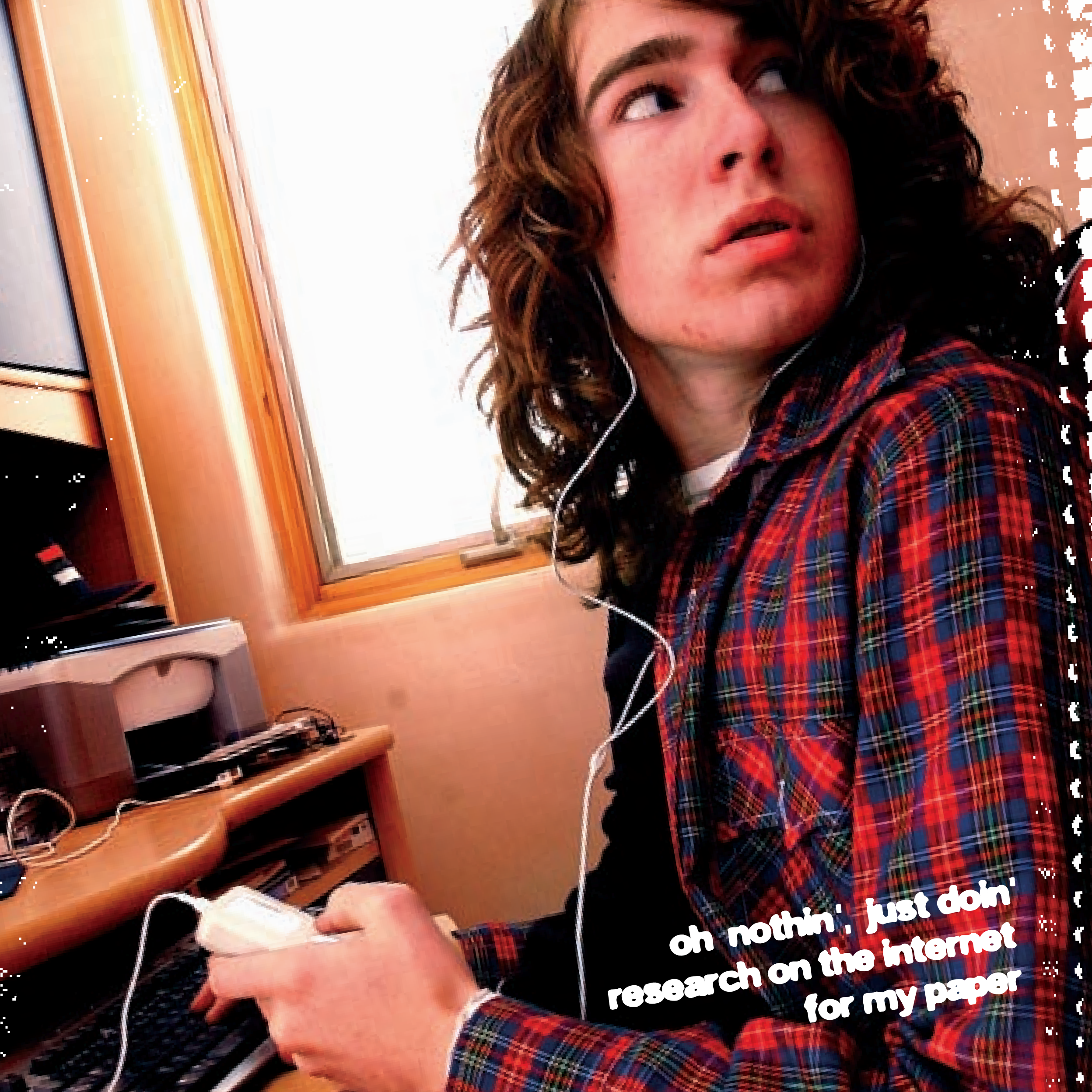
What does your child not want you to see? Are they ashamed of something? Talk to them about their online activity. Be aware, though, that prying too much could foster paranoia in your child and lead to more secretive behavior and further isolate themselves from you.

4. You find pornography 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

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 predators 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 a cyber predator, go to websites like:
www.mcctf.org
www.thelost.org or
www.missingkids.com

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

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

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.

Let them know that there is no reality on the Internet. 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. See the section on Tools for more information.

ONLINE ACTIVITIES and their POTENTIAL CONSEQUENCES:

1. Filling out online profiles

Filling out profiles will allow predators to see personal information about your child, such as their real name, phone number, address, school name, etc. and will allow the predator to "find" your child in real life.

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 online predators a more intimate look into your child's thoughts and feelings. By reading postings on a blog, a predator can get a greater insight into a child's vulnerabilities, likes and dislikes and can "tailor" his message to target the child. Even though this may take longer for the predator to learn about the child, the posting of the child's thoughts and feelings give the predator 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 a predator, 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 them through that window. Predators will 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.

AGE APPROPRIATE GUIDELINES

The rules and guidelines that you establish for young kids, preteens and teens will most likely be very different, much like the way that rules for crossing the street are different for children of different ages. 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 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 and a predator may tell you 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 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 will not tell anyone!

... k fine. I will tell dad about you chatting with the weirdos all the time.

HONEY...
I'M JUST TRYING TO PROTECT YOU.
.. 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 without invading their privacy. Make sure they still feel comfortable talking to you about what they do on the Net.

- **Don't talk down to your teen.** Instead, show your teen that you trust them to make good decisions. **Encourage them to protect themselves from online predators by being vigilant and cautious.**

- **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 what it was like to be their age. 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.** Let them know **what you consider inappropriate.**

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 Maine Computer Crimes Task Force (www.mcctf.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 1-800-871-7741.

INTERNET SAFETY TOOLS FOR PARENTS

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

- **Computer Placement**
- **User Profiles**
- **Web Browser Controls**
- **Viewing Internet History**
- **Filtering/Blocking/Monitoring Software**
- **Filtered ISPs**

Computer Placement

Keep the computer in a common area of your home. It's easiest to monitor what your children are doing without having to pry if the computer is in an open area of your home, such as a living room, a loft, or the kitchen. Don't place the computer in a room where your child can close the door and go online.

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

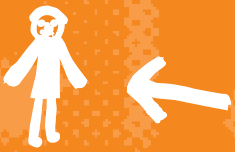
In order to track your child's online activity, you can use the Internet History and Temporary Internet Files to see what websites have been accessed recently. More savvy computer users can easily delete this information from easy access, but this information is still typically accessible by a computer expert. For more information about viewing Internet history and temporary Internet files, consult your browser's help files.

Software

There are many different software programs available for purchase that 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
- Operates 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

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.

SUCCESSFUL FRAUDS AND SCAMS LOOK LEGITIMATE. Don't let an authentic-looking email that appears to be from your bank or credit card company fool you into revealing your personal information.

KEEP YOUR FINANCIAL INFORMATION SECURE. 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.

BE CAREFUL WHEN SELLING ITEMS ONLINE. Be suspicious if someone sends you a check and asks you to wire money back.

PAULA D. SILSBY
United States Attorney
District of Maine

WINNING A LOTTERY won't happen if you haven't entered. And no legitimate lottery asks you for money in order to collect your winnings.

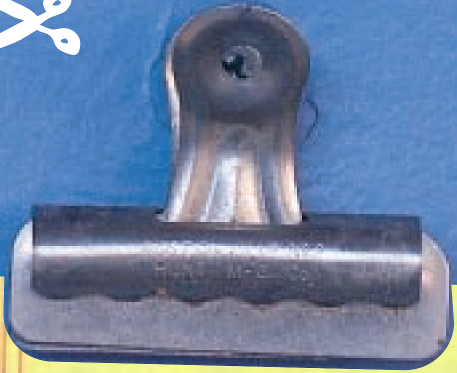
RESPONDING TO EMAILS that ask you to respond (or your account will be closed) are typically an attempt to steal your personal financial information.

"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.maine.gov/ag/ and click on Consumer Protection