Protect Yourself!

SOCIAL SAFETY

A Public Service By:

myyearbook

Did You Know?

- **22% of 16 - 17 year olds had a face-to-face meeting with someone they met online.**
  (NCMEC - National Center for Missing and Exploited Children)
- **1 in 7 teens have been sexually solicited on the Internet**
  (Online Victimization of Youth: Five Years Later, NCMEC, December 2006)
- **1 in 3 have been aggressively pursued sexually online.**
  (CyberAngels)
- **One in 11 minors have been threatened or harassed online.**
  (CyberAngels)

What's Inside:

STUDENTS:

Go to www.SocialSafety.org for more info on how to protect yourself, what to look out for, and how you can help.

PARENTS/EDUCATORS:

www.SocialSafety.org provides answers to tough questions like how to approach your kids about online safety.

Beware! Predators!!

It's really easy to be someone you're not on the Internet. After all, who's going to know if you add a couple inches to your height, use a different picture, or add a couple zeros to your net worth? You can be funnier, cuter, more confident: the ideal version of you. But guess what? If it's easy for you to be someone you're not, it's easy for someone else as well.

Anyone who's ever seen an episode of Law & Order or CSI knows there are people who use the Internet to meet kids for purposes that are not totally kosher, and they're not always that easy to spot. They're really good at what they do: **making friends with and trying to seduce kids into meeting them for sex. A predator could rape you, kidnap you, or kill you.**

Sometimes the guy pretends to be a kid, trying to meet you on your level. He could have a tricked-out profile with music, videos, and a pic of an attractive teen next door. Or he might come right out and say he's 35, 47, 68 years old and thinks you're the sexiest thing ever.

That should send your Skeev-O-Meter right through the roof. Remember this person may intend to rape or kill you.

To Catch A Predator ...

There are several ways to report an online predator:

- **If you think there is a threat** to your safety or well-being, call 911, or let your local police know immediately. Let them know that a stranger has threatened you online, and that you would like to make a report. You will never get in trouble for making such a report, even if it turns out the predator wasn't for real.
- **Submit a report to the CyberTipline.** The CyberTipline is an agency that was created by the United States Congress to take reports of abusive behavior towards children on the Internet. Reports can be submitted anytime 24/7 at cybertipline.com, or toll free at 1-800-843-5678.

And there are a lot of these guys. **Did you know that 1 in 5 kids say they've been sexually solicited on the Internet?** These guys prey on kids who are unsure of themselves, eager for attention and spend a lot of time online.

So all of us, basically.

So if you don't want to be the next *Law & Order: Ripped from the Headlines*, there are some things you can do.

- **Remember people aren't always who they say they are.** That cute sophomore you met the other day could be a fifty-something year old man with a weakness for a 14 year old. It's more than possible. So watch what you say online.
- **Don't post personal information or revealing pics in your profile.** Once an image or bit of information is put online, you can't control it. Your pic could end up on a pedophilic porn site, your face could be photoshopped to a porn star's body and emailed all over, your mom could find it.
- **Call 911. Call 911. Call 911.** That's what the number is for! Notify the police immediately if an adult tries to send a sexually explicit picture to a child or tries to get a sexually explicit picture from a child. If you ever feel uncomfortable with any conversation with an adult, notify the police.

Dealing with Bullies

Cyber bullies are a new breed of the old schoolyard jerk, but instead of beating you up for your lunch money or pushing you in the mud, they use the Internet to harass you. These jerks use the Internet to harass people they don't like, friends they're mad at, or total strangers. Cyber bully attacks are double scary because a lot of the time, you don't know where they're coming from. It's like getting sucker punched in the dark.

Cyber bullying comes in a few guises. There are the one-on-one messages. Or someone could distribute your personal information or embarrassing photos through emails or postings on a website. Or someone could actually be trying to hack your computer or website through viruses or DOS attacks or something else.

Being bullied hurts all the time, whether it's in the real world or online. If you're getting harassed online (or offline), **here are some things you can do to make it stop.**

- **Call Someone.** Victim advocates associations like the Stalking Resource Center (800-FYI-CALL) or Safe Horizon can help you assess threats and explain your legal options. **If you sense a threat, call 911 and get law enforcement immediately.**
- **Block the harasser.** It is the easiest way to knock out harassment but does not always work.
- **Create a new identity** by deleting your old profile, blog, email, or IM accounts and making new ones. Sure it's a bit of a hassle, but it's worth it.
- **Document the harassment.** All text, IMs and emails should be saved to show to the proper authorities if the harassment continues.
- **Ignore them.** Really, it sometimes works. Most bullies are trying to get a rise out of you, so don't give it to them! Block their IMs, delete their emails, and take them off your friends list. If you don't give them a reaction, they might get bored and move on.
- **Don't Post Personal Information** like your cell number, your IM name, or your email address. It's bad enough that some creepy person is probably looking at your personal profile already. Do you want to give them even more access to your life? How annoying would it be to have to shut down your email account, get a new IM name or phone number because some psycho is harassing you? This one is so easy to avoid. All your good friends will probably have this information anyway.
- **What you post will remain** - Remember that everything that you put online could be accessed by anyone, anywhere. What do you really want people to know about you?

Big Bully: Are You a Cyber Bully?

So what is a cyber bully exactly?
If you have to ask, it might be you.

Here are some typical Cyber Bully behaviors:

Flaming: Flaming is the posting of derogatory remarks on someone else's webpage or IMing nasty remarks to someone. Mostly, it's online fights filled with bad language. The best way to deal with flaming is to ignore it. Take down the post or block the person on IM. If you fight back, you're engaging in a flaming war and are just as guilty as the person who flamed you. Flaming wars can escalate into real life physical fights, which nobody wants. Call 911 if you are threatened.

Impersonation: Impersonation is when a person logs into someone else's account and sends out messages pretending to be that user. Guess what? This is a form of identity theft! If this happens to you, call the police immediately.

Bad Mouthing: This can include creating profiles that make fun of another person, erecting blogs that rate people in your class or creating home pages that make fun of others. This can be taken very seriously by authorities. In her book, *Totally Wired: What Teens and Tweens are Really Doing Online*, author Anastasia Goodstein tells the story of one Michigan parent whose daughter was expelled from school when she created a MySpace page that bad mouthed her home economics teacher.

Hello Blog, Goodbye Job!

So, you think you know who's looking at your blog or profile? Sure, your friends, their friends, your cousin, his friends, random websurfers, no one you need to worry about. It's not like they'll think any less of you for all the stuff you've got posted there. Right? Wrong.

Ok, so try this: your teachers, the cops, college admissions counselors, your boss, the director of that internship you want, **your mom**. A lot of employers now will check out your MySpace before they hire you!!!! There are no stats on admissions officers, but you can bet they are checking it too.

Did you hear about the kids who got arrested for burglary when they posted about their exploits on their MySpace? How about the kid who got busted for possession when he posted pics of himself hitting a bong?

To make up for their lack of experience, police, teachers, and guidance counselors have been getting training in navigating sites like MySpace and deciphering the blogosphere. What's more, a lot of colleges and employers are looking at kids' blogs and profiles before sending out acceptance letters and interview invitations. And if you've already snagged an internship or admission to the school of your choice, what you post in your blog could get you fired or expelled.

So, if you post something stupid online and get rejected or canned because of it, you (unfortunately) have no one to blame but yourself. We can debate whether it's appropriate for companies and colleges to use dirt from the Internet in hiring and admissions, but the fact is they're doing it, and that means we have to be careful.

Here are some things you can do to cover yourself:

- **Don't post stupid things online.** Like that bikini pic of you, without the bikini? Don't post it! Or that lengthy blog entry about how much booze you drank. Don't post that either!
- **If you absolutely must must must** post the exposés of your life, lock them so they're Friends Only or Private. But remember that even locked, there's still a chance someone you don't intend to see it could view it. In fact, there's more than a chance. **It will happen!**

More and more admissions officers are checking your MySpace.
"At least one college applicant was denied admission because of their blog."
- NACAC

Malware and Viruses

Pretty much everyone knows the basics of protecting their computer from the packs of malware that prowl the Internet. Firewalls and other security software can zap most of the ambient junk that your computer picks up just by being online. But some of the more sophisticated viruses and bits of bad code can still slip through and muck with your system.

So what is malware exactly? Malware is a software designed to infiltrate or damage a computer system. It is often referred to as badware or computer contamination. The different forms of malware include trojan horses, spyware, worms and dishonest adware.

- **WORMS:** Worms were originally designed to destroy files on a hard disk, or to corrupt the file system by writing junk data. Now hackers are using worms to turn people's personal computers into zombie computers (or computers that are unconsciously part of a network) to issue spam or perform other malicious acts. Worms scan computer networks for computers with vulnerable network services, break in to those computers, and copy themselves over.

- **TROJAN HORSE:** A Trojan horse is a program that invites the user to run it, but conceals a harmful or malicious payload. The payload may take effect immediately and can lead to many undesirable effects, such as deleting all the user's files, or more commonly installing harmful software into the user's system so that hackers can get into your system often.

- **SPYWARE:** Spyware programs are commercially produced programs used to gather information about computer users, showing them pop-up ads, or altering web-browser behavior for the financial benefit of the spyware creator.

Below is a list of ways you can prevent viruses and phishing on your personal computers:

- **DON'T FILE SHARE:** A lot of viruses are issued through P2P sites like Kazaa, Morpheus, iMesh, eDonkey, Gnutella, LimeWire, and Grokster accounts for thousands of illegally downloaded music files, games, movies and software. Even if those sites are innocent, many are not.

- **DON'T OPEN ATTACHMENTS FROM UNKNOWN EMAILS:** This is the number one way that hackers can get into your system.

- **DON'T OPEN SPAM:** When spam comes in, the best idea is just to delete it immediately. Never buy a product from spam or click unsubscribe. It is an easy way for hackers to gain entrance into your computer system. If an email address is attracting a lot of spam, create a new email account.

Protect Your Password: Don't be a victim of phishing

Another big concern lately is phishing. Phishing is when a hacker attempts to get your usernames, passwords or credit card details, by pretending to be a trustworthy source, like an email or a bulletin board post on a social networking site. Here are some tips on how you can avoid being phished:

Create Intricate Passwords: Use passwords that are at least eight characters long that include at least one numeral and one symbol. The more difficult a password is, the less likely it is to get phished. Never disclose a password online.

Avoid Filling Out Forms in Email: It's difficult to know where the data will be sent and the information can be intercepted several stops along the way to the recipient.

Never Click on Links in Email or IMs: If you need to visit a website, go to the business's site directly.

Use a False Password on Your First Login Attempt to a Site: This is a good way to test the validity of a site. If you get an error message, then it means the site didn't find your password in its genuine database and will alert you to the fact.

Make sure you clean up your system a couple of times a month. Run Disk Defragmenter and Disk Clean Up. Minor malwares and trojans that aren't problematic enough to cause any real damage on their own can still eat up a lot of memory if they pile up, and crash your system that way. Investing some time and money in making sure your PC doesn't turn into the ravenous undead isn't such a bad idea.

"The average computer is attacked by malware within six seconds of going online."

Parents and the Internet

POS... TTYL
Parents are a joy when you're a teenager, aren't they? Always asking you where you're going, when you'll be back, who'll be there, on and on, blah blah blah blah. And now, with the rush of Internet safety stories in the news, they have something new to freak out about: what you do online.

When I first started playing around online (I was about twelve), my parents wouldn't let me have an Internet computer in my room and insisted on looking over my shoulder at everything I did. They got bored of that pretty fast, and instead tried to install tracking software and a keylogger so they could keep tabs on where I was going and who I was talking to.

I talked to my parents about it. I told them what sites I went to and what they were for. We talked about who I chatted with online, and they gave me some kids-only sites where I could meet people my age. Yes, I had a blog, and yes, they could read it. I didn't post anything dangerous on it anyway.

Nothing to LOL about ...

AITR = Adult In The Room
P911 = Parent Emergency
PAW = Parents Are Watching
PIR = Parent In Room
POS = Parent Over Shoulder
PLOS = Parents Looking Over Shoulder
PRW = Parents Are Watching
MOS = Mom Over Shoulder
PAL = Parents Are Listening
CD9 = Code 9 - (means parents are around)
MIRL = Meet In Real Life
LMIRL = (Let's) Meet In Real Life
ASL(R P) = Age Sex Location (Race / Picture)
E or X = Ecstasy (the drug)
S2R = Send To Receive (pictures)
TDTM = Talk Dirty To Me
GNOC = Get Naked on Cam (web cam)

My parents admitted that I was being much more mature than they had expected, and though they thought that some things online weren't appropriate for how young I was, they decided to trust me more. When I turned 18, I got a brand new laptop that I could take to college.

So your parents are totally clueless about the Internet?

NO SURPRISE!
Here are some websites you can send them to teach them things they need to know about the Internet:

SocialSafety.org: A useful guide to online safety for teens and social networking safety.

WiredSafety.org: All-inclusive, free resource focusing on Internet safety, help and education for Internet users of all ages.

MissingKids.com: The National Center for Missing & Exploited Children.

Talk to your parents about the Internet. Tell them the kinds of things you do online and the steps you take to keep yourself safe. Pass on this booklet so they know you're dealing with online dangers in a responsible way. Mostly, your parents are just worried and want to make sure you're alright. This makes them overreact sometimes when they're trying to protect you from something they see as a threat, but the threat is real. Bad people rape & kill kids and teens. It's all over the news. Do your best to convince them that you are aware of what's going on, and you're handling yourself responsibly. And if they still come down on you hard and banish the Internet from the house, or whatever, you just have to suck it up and do what they say. They are your parents, after all. And how long do you have to wait before you go away to college, anyway?

Report Violence and Self-Harm

Being a teenager is scary, stressful, and confusing. It's sort of like being trapped in a jail for eight straight years. The Internet gives kids who are in trouble lots of places to go for help, and it also gives them a bunch of opportunities to ask for help if they need it. If you find one of these cries for help on a friend's blog or in a chat room, you'll probably want to help, but you'll probably also be a little freaked out and not really sure how to help.

Here are some things to do if you find someone online who's threatening to hurt or kill themselves, or who you think might be in danger:

- **CALL 911:** Ok now, this bit is really important: If you believe the person is in immediate danger of hurting themselves, call 911 immediately and tell the operator that you want to report a suicidal person. If you can, tell the operator exactly where the person lives. If you can't, give as much information as you can: full name, age, gender, general location, screen names, email addresses, IP address, where the threats were posted, and anything else you can think of.
- **Right away, call the person** if you have their phone number or find some other way to get in touch with them through emails or IMs or whatever. It's important to get them to talk about what's wrong and make sure they know they're not alone.
- **Tell someone!** Talk to your school guidance counselor, your favorite teacher, your pastor or rabbi, or even your parents. They'll be able to help you make sure the person is ok. If you've been asked to keep suicidal behavior secret, don't! Some secrets shouldn't be kept.

Facts About Suicide

If you look around a class of 25 students, at least five are likely to have seriously considered suicide, and at least two are likely to have tried to kill themselves in the past year. Scary, huh?

THAT'S NOT ALL:

- Almost 1 in 5 had seriously considered attempting suicide.
  (Centers for Disease Control and Prevention)
- More than 1 in 6 had made plans to attempt suicide.
  (Centers for Disease Control and Prevention)
- More than 1 in 12 had made a suicide attempt in the past year.
  (Centers for Disease Control and Prevention)
- 90% of teen suicide victims suffer from depression, and/or have a history of alcohol or drug abuse.
  (Journal of Consulting and Clinical Psychology)

If you are feeling depressed or know someone that seems suicidal, tell someone before it is too late.

Suicide is the third most common cause of death for American teenagers, after accidental injury and homicide. The Surgeon General says that someone in America commits suicide every two hours. That's pretty freaky, but the good news (well, good in a still depressing way) is people who are suicidal almost always show some warning signs beforehand. They could be more withdrawn or depressed than usual, talk about suicide and death, or start giving away their possessions.

If one of your friends seems suicidal, do everything you can to make sure they get help, even if they say they don't want help or that you're worrying too much. In situations like this, it's a whole lot better to be safe than sorry.

Preventing Another Columbine or Virginia Tech at Your School

Did you know that each of these shootings could have been prevented? No joke. Eric Harris, one of the shooters at Columbine, set up a blog nearly three years before the massacre that spoke of his plans. Seung-Hui Cho of VA Tech had been reported by an English professor to the campus counseling center.

Here are some things that you can do to help prevent such a tragedy from occurring in your school:

Take Threats Seriously: If you read threats of suicide or violence on a blog or profile, forward the link to your local authority. Aside from call in hotlines to report crimes, most local police stations now have personal websites. Log on and report the blog or profile to the police or call 911.

Encourage Your School to Have a Tip Box: The Jefferson County School District, which includes the Columbine school, now has an anonymous tip box, where students can submit reports about threats or violent behavior of other students. This has promoted an atmosphere of school safety.

When using a social networking site, look for the Report Abuse! icon.

This icon, developed by the New Jersey Attorney General, allows you to quickly report abusive behavior and sexually inappropriate materials to the operator of the social networking site. Site operators using the icon have agreed to review all reports and alert law enforcement about possible predators.

Remember, however, that the Report Abuse! icon is NOT a 911 line to the police. Call police immediately if, for any reason, you feel that you or someone else is in danger or has been threatened by someone online.

To learn more about the Report Abuse! icon please go to www.NJPublicSafety.com/reportabuse. If you know of a social networking site that wants to use this icon please contact the New Jersey Attorney General's Office at the following email address: citizens.services@lps.state.nj.us.

** The State of New Jersey and the Attorney General's Office has no control over, and is not responsible for, the content of the SocialSafety.org educational packet.*

NJ Attorney General