

What is Net Literacy? It is a nonprofit "youth empowered" organization that benefits from the experience of adult mentoring and direction. The Net Literacy Corporation has five digital inclusion programs, and this is our Safe Connects program specifically designed for elementary school students and their families.

We are grateful that the Indiana Department of Education, principals, law enforcement officers, and parents review our "student created" presentation – but Net Literacy is responsible for the content.

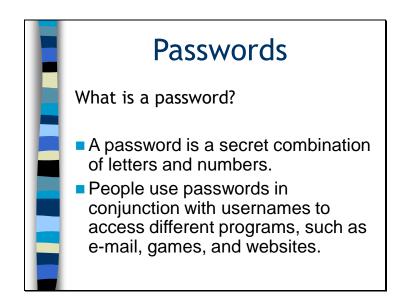
Our mission is to provide Internet and computer safety education to students, family members, and senior citizens.



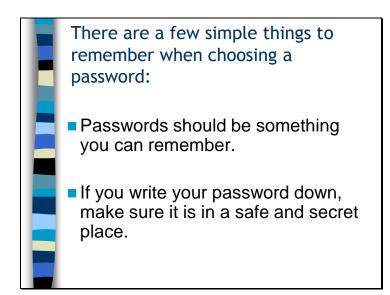
Today you'll learn how to stay safe while using the Internet. We'll discuss topics including passwords, net predators, profiles, netiquette, e-mail, viruses, chat rooms, and community websites.



We will start today's program by discussing passwords.



Many of us has heard of the term, "password, but what does it really mean?





Okay, now that you know about passwords - I want you to tell me if these are good or bad passwords for a student named Andrew Smith. Let's go through this together.

Secret1 – Okay is Secret1 a good password...it's not so good because it's easy to guess. Mypassword – What about Mypassword...it's not so good because it's also easy to guess.

Asmith – How about Asmith? Bad...because it's just Andrew's first initial and his last name – to easy to guess.

F3d20w9 – What about F3d20w9. Whew! It's good – if you can remember it – no one would ever guess it.

Andrew – And what would you say about Andrew? If you said it's too easy to guess and a bad password – you'd be right.

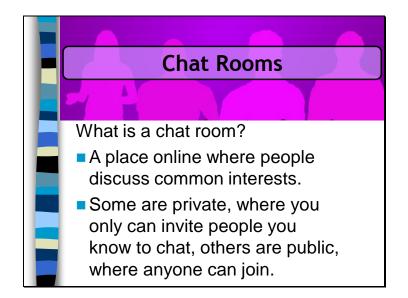
Password1234 – Okay, for Password1234, you're right if you said it was too easy to guess. Freethepanda – Freethepanda – that's just a made up word – so that's a good one – tough to guess.

Smith – Okay, what about Smith? For everyone that said "too easy," you'd be right! Pokadots – Pokadots – is a good password – if it's a word that you just decided to use and doesn't have any special meaning.

Safeconnectsrox – And lastly, Safeconnectsrox – it's a good name because it's true but more importantly, no one would ever guess it.



Let me tell you a few things about chat rooms, private chat rooms, and instant messaging – sometimes called **"IM."**



A chat room is a place or location online where people can discuss a common interest. **Just like any other place**, the Internet has good and bad people, **so you have to be careful**. Some chat rooms are "private" and are entered by invitation only, while others are open for anyone to join. First, **never** accept an invitation into a private chat room unless it's with a friend you know well. Public chat rooms can also create problems.



If you are in a chat room with others who make you feel uncomfortable, **leave it**. "**It's as simple as that!**" When you're in a chat room, you really don't know who you are talking to. Are they a friend of a friend or a complete stranger? Strangers on the Internet and chat rooms can be dangerous, and **it's not worth getting involved**. We strongly encourage that you don't participate in public chat rooms because anyone, "*anyone!*", could be talking. If worst comes to worst, and you feel threatened, just turn your monitor off and talk to your parents.



Some people go into chat rooms just to cause trouble and be mean. This is called **"chat room bullying."** Comments can be made about your race, religion, if you're a girl, a boy, or **for no reason at all**. They probably don't even know who you are – some people get their kicks by just being mean.

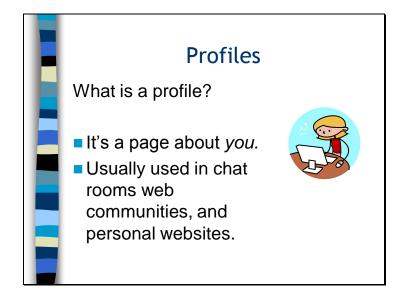
Instant messaging is a one-to-one voice or text conversation that is available through the Internet. If someone tries to Instant Message you and you don't know them – don't answer them, just like you wouldn't talk to strangers in real life. And remember, you can't see or hear this stranger – so don't IM unless it's with a friend that you already know.

If worst comes to worst, and you feel uncomfortable or threatened, just turn your monitor off and talk to your parents. Most importantly, if someone who talks to you online asks to meet you in public, **don't meet them**, and be sure to, tell to your parents.



Now we're going to talk about profiles.





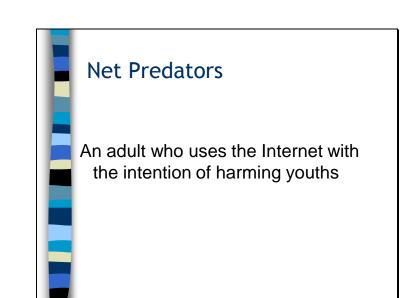
A profile is a page where you tell others about yourself and is usually used in chat rooms, web communities and personal websites.



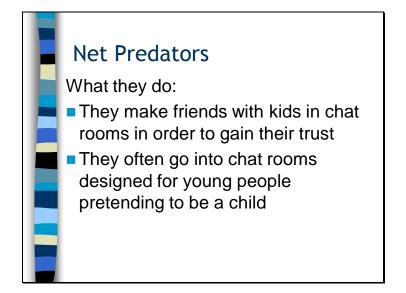
Some people write profiles and others choose not to. Talk to your parents if you want to write a profile and see what they say. Sometimes writing a profile can put you at risk. If your parents agree that it's OK, we recommend in your profile, you talk about your favorite hobbies, TV shows and games, but NOT about your personal information. Don't include your full name, family information, and **NEVER** include your address **or** phone number. Remember, before you consider writing a profile; discuss this with your parents.



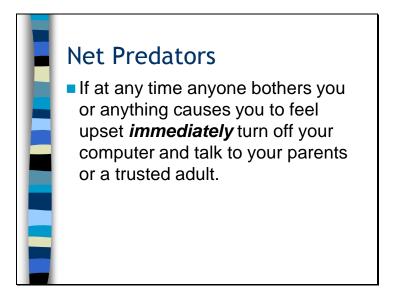
Next let's talk about Net predators.



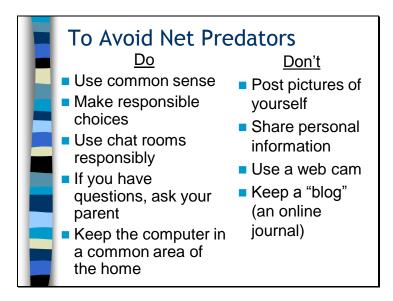
What is a net predator? A Net predator is an adult who used the Internet with the intention of harming youths. I'm sure you've been told not to talk to strangers when you go out in public, well; the same rule applies to using the Internet. Not everyone online is a good person; sometimes there are people who do bad things, such as Internet predators.



Net Predators often go into chat rooms pretending to be children in order to gain their trust. Remember, the internet is a pretty anonymous place. Anyone can pretend to be anything.



If you feel threatened, or if anyone bothers you, what to do is simple: Turn off your monitor and talk to a parent or a trusted adult.



There are a few simple things you can do to avoid becoming a victim of an Internet predator: Use common sense and make reasonable choices. Avoid sharing personal information such as full name, address and telephone, and don't post a picture of yourself. If you ever feel unsafe, or know that someone online is doing something wrong, again, talk to your parents or a trusted adult.



Now let's talk about language and conduct on the Internet.



Having a conversation online is just like having a conversation in person or on the phone. Just because the person can't see you, doesn't mean that you can act differently; it's still important to be polite.

On the Internet, being polite and using good manners is called Netiquette or "Net Etiquette."

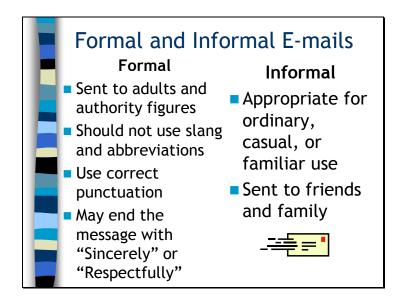
Here are the rules of the Internet for using good Netiquette:

- Only type something that you would say to a person's face
- No swearing or offensive comments because someone's feelings may be hurt

- Facial expressions are not able to be read on the Internet, so make sure to let a person know when you are joking; do not joke in a potentially offensive way



Here are a couple of examples of how to act on the Internet; it's just as applicable to the real world. If you disagree with someone, express your opinions respectfully. Typing in all capitals means that you're yelling and may hurt someone's feelings. Don't use your computer to harm others! This includes taking passwords and files that belong to others, or spreading viruses or rumors. Overall, just treat people online just like you would in real life – just treat others as you'd want them to treat you.



What's important to know when writing emails?

You know that writing letters and talking to friends is different from talking to your parents or to your teacher. When typing an e-mail to an adult or other authority figure you should use proper grammar, punctuation and avoid using slang. When sending e-mails to your friends you can be more casual and relaxed.

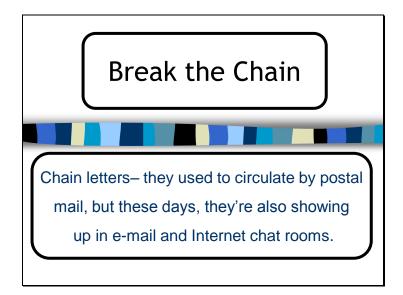


Our next topic is chain mail – which is junk mail, hoaxes, and people trying to sell you stuff over the Internet.

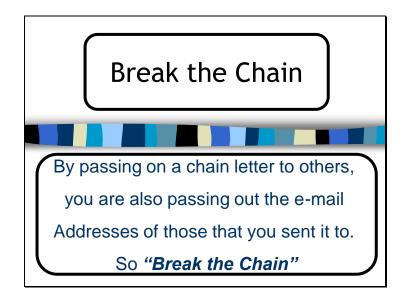


Have your ever been sent a chain letter?

You probably recognize one when you see it: With subjects ranging from friendship to religion to good luck, you're supposed to e-mail the letter to a specific number of other people with directions on how they should "continue the chain." Usually a chain letter threatens consequences to those who don't pass the message on.



People used to send chain letters in the mail, but now they send them using e-mail. These letters focus on many different topics – such as hoaxes, rumors, jokes, but the main idea of all chain letters is to pass it on to a certain number of people in order to keep the chain going.

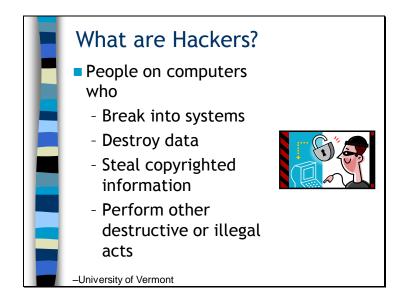


The problem is that when you pass on a chain letter you are also passing out the e-mail addresses of the other people that you sent it to, making it easier for them to get computer viruses. So when it comes to chain mail – break the chain and don't forward chain mail on to others.



Let's discuss hackers.





Hackers are individuals that break into computer system to create trouble. Sometimes they destroy data, steal copyrighted data, or just try to create problems for no particular reason at all.



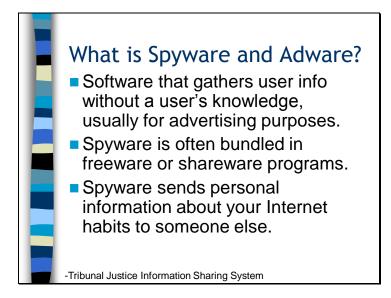
Sometimes Hackers use the data that they steal for identify theft. They obtain confidential information, such as your credit card or social security number, use this information to obtain a credit card, and buy things that are charged to you. Through the use of bad computer programs, they can destroy data on your computer – or make your computer act unpredictably. Sometimes, their Trojan horses, viruses, and worms can turn your computer into what is called a zombie computer. Upon command – it will attempt to access a particular site hundreds of times each minute. When tens of thousands of these zombie computers do the same simultaneously, it's called a denial of service attack because sometimes the website, such as CNN.com, is so overwhelmed by these all of these accesses attempts that it will prevent legitimate users from being able to access the website. And that's a denial of service.



These are the three things that you can do to protect yourself from hackers. Always make sure that you have a firewall, which is software that you can purchase that prevents anyone from accessing your computer via the Internet without your permission. Always make certain that you use antivirus software and ensure that you keep it-up-to date. And limit the amount of personal information that you keep on line, because hackers can use it to help them steal your identities and run up credit card debts in your name.



What is Spyware and Adware?

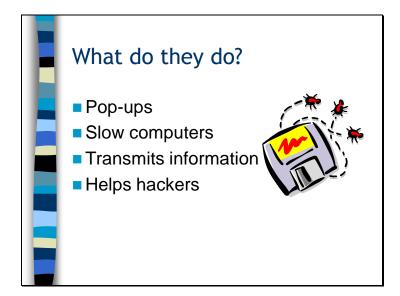


•Any software - that gathers user information through the Internet without their knowledge, usually for advertising.

•Spyware applications - typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet.

•Once installed, the spyware monitors your activity and sends that information to someone else undetected.

Basically, both types of programs track anyone that uses your computer. Adware shows advertisers how you use the Internet – so they can try to sell you things by placing ads for things you like or to test their advertising. They usually don't know exactly who you are – but gather information from millions of computer users. They do slow down your computer. **Spyware is much more serious** – once it is on your computer, it can secretly figure out your passwords, then it can send your passwords and other private information to the person that created the spyware.



Spyware and adware creates problems. As we discussed, it transmits information from your computer which can help hackers. Adware can also create pop-ups, which are ads that pop-up on your computer in another browser window. All of these extra spyware and adware programs are annoying and slow down your computer.



How do you get Spyware and Adware and how can you protect yourself against them?



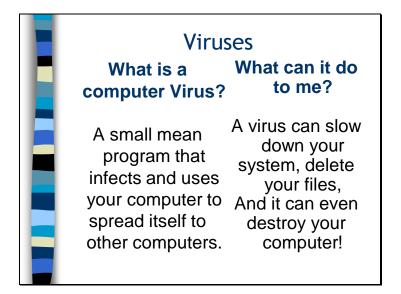
Here are the four ways to get spyware and adware. Let's say you get an email that asks you to go to a website that you have never heard of before – if you go to that site – even if you don't click on anything, a spyware or adware can be secretly downloaded into your computer. That's why having a firewall is so important. Don't download a program or open an email attachment unless you are certain that you know who it is from and that it is doesn't contain a virus, worm, Trojan Horses, or other program that could install adware or spyware on your computer. Stick with toolbars from reputable companies that you've heard of before – such as Google.com.



We have discussed hackers, viruses, spyware, and adware – and now know that antivirus software and a firewall should be installed on every computer. Also, there are free versions of programs like Adaware SE and Spybot that can be downloaded via the Internet – and will help computer users keep spyware and adware from taking over their computer. Adaware SE and Spybot: Search and Destroy can be found on the Internet at www.download.com or by conducting a search on these products. The free versions of anti-spyware and anti-adware software should be run every couple of days – since they do not automatically eliminate spyware and adware does.

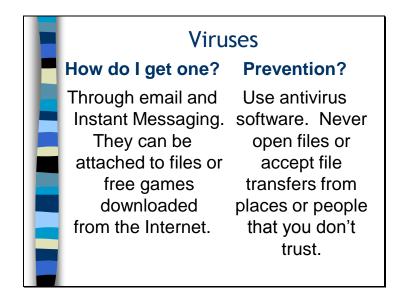


Now we're going to discuss destructive ways that some people will use to try to break or cause you to lose all of the information you've stored on your computer.



What is a virus? **"I bet you guys are thinking of a cold or the flu." "No really, in this case"** a virus is a small malicious (mean) program that infects and uses your computer to spread itself to other computers. Viruses are sneaky and people usually don't even know when they have one

And what a virus can do can cause you lots of problems. A virus can do almost anything to your computer. It can slow down your system, delete your files, and make your computer act weird. It can also **even** destroy your computer! Be afraid... Be very afraid ⁽²⁾ Viruses are unpredictable because each virus can impact your computer differently. But they can ruin your computer or corrupt your files – and new viruses are released every day.



Viruses spread when you open a file attached to email, through Instant Messaging, or by downloading games or programs that have a virus implanted in them.

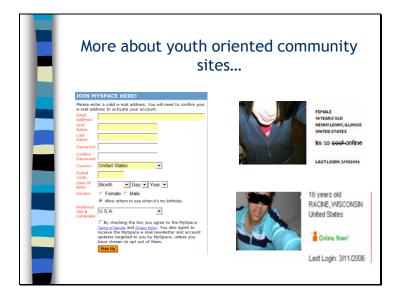
So how do you prevent a virus from infecting your computer? First, make sure that you have anti-virus software on your computer and keep it up to date so your subscription doesn't expire. Secondly, use common sense. Be as careful on the Internet as you are when you cross the street – since we know that viruses are out there – use good judgment and don't open anything from someone you don't know. Even if a friend that you know sends you an email that seems strange or out of character (such as them sending you an attachment that says "**YOU WON**") – don't open it - call them first to check that it was really them that sent it.



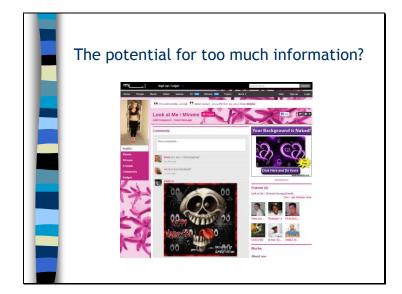
What are community websites? They are websites where people go to meet other people, tell others about themselves, and develop a virtual web-community. However, community websites have the potential of providing others too much information about yourself and can create a dangerous environment. Let's talk more about what web communities are and how they can be dangerous.



Just like in real life, there is good and bad on the Internet. Sometimes, websites that were not created for harm get used for unintended purposes. One group of websites that falls into this category includes community websites. There are many community websites out there including Myspace, Facebook, and BlackPlanet, just to name a few. Myspace is one the more popular web-community on the planet, having about 100 *million* members, and Facebook has over 600 *million* members. Since many teens use MySpace, I'll tell you a little about them. They make changes to their site all of the time, but here's a copy of their home page.



Most of these web-communities target teenagers and individuals in their teens and 20's. When registering for an account at MySpace, you have to fill out forms with your name, your country, your gender, your e-mail address and your date of birth. If the computer realizes you are 14 or younger, you will be denied an account. But that doesn't mean that students don't "pretend" to be 15, 18 or even 21 for that matter. The fact is, many pre-teens lie when they register, so that they can join their "friends" online.



Once you register you fill out a bunch of boxes and fields with interests, occupation, hobbies, a picture etc. The website uses this information to help users find and talk to old friends, and meet new friends. But, of course, this functionality presents risks to the uninformed. If you are in 4^{th} , 5^{th} , or 6^{th} grade, here's a good rule to follow before deciding to join a community website – first talk it over with a parent or a trust adult. They can help you decide if it's right for you. If they say it's okay, ask them to look at your online profile to make sure that you are safe.



Navigation on these community websites is easy and users can move from person to person and picture to picture through hyperlinks and clicking on images. Pictures are really popular on these websites, and since parents don't always moderate what is put up on the Internet, sometimes disgusting pictures are posted. This creates an opportunity for Internet predators – especially because a person's site can combine pictures, blogs, profiles, and personal information all in one location. MySpace, Facebook, BlackPlanet, and the other community websites try to make sure their websites are safe...but it's not always easy for any website to do this – just like no matter where you live – there may be some places that are not that safe after dark.



Let's talk a little more about community websites



MySpace, Facebook, BlackPlanet, and all other community websites are not good or evil – they are a microcosm of what's on the Internet. I guess no site can be correct all the time – especially if they allow any youth to have the freedom to post information about themselves. If you use MySpace, they have good information about how to protect yourself and keep yourself safe. Check it out...and discuss the safety tips with your parents.



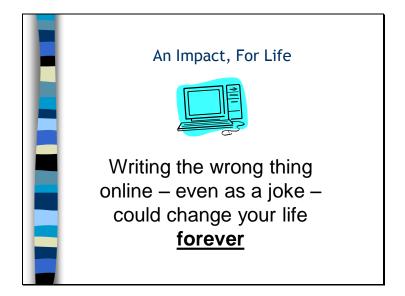
Frequently, these web-communities put out surveys and questionnaires that users fill out to match up people with common interests. These questions are also sometimes posted on a user's profile. Questions can go way beyond "what's your favorite color," and "who's your favorite sports team." But questions dealing with drugs, shoplifting, being beaten up, and physical relationships are far too common. If you answer these questions truthfully, you might disclose information you'll later regret. What's worse is if you lie about something online, people will accept it as true because they can't hear your sarcastic tone or see your silly grin. It's so easy to lie and put things on these websites that are completely not you. It's scary. And the sad thing is a lot of people do it. Most youth-oriented community websites have these questions that are designed to keep members on the site – but if a family decision is made that community sites are okay – use good judgment and talk to your parents about what questions you to answer.



In addition to profiles, there are also forums, chat groups, and blogs on most web communities – and on many other sites too. Many forums and chat groups are educational or reflect what teens want to talk about – but like anywhere on the Internet – (and this is not a reflection on any particular youth oriented community group) – anyone can find whatever they are looking for – or sometimes what they're not looking for - online. Blogs, also known as web-logs, are also common nowadays, and are completely available to the public. They're essentially a diary, online. I know that if I had a diary, I wouldn't want to post it online. But it's becoming the "norm" and it's a huge privacy threat. Think about the kinds of personal information you want to share with the world.

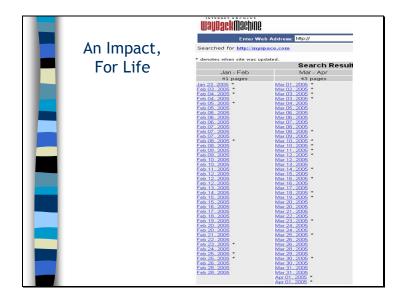


Let's talk about how too much information can get you in trouble.



We've heard about the different ways information can be posted on the Internet – and now we'll discuss how something done today could impact **you** *for the rest of your life*.

More and more frequently, employment departments and colleges are checking community websites to see if you have an account, and if there is anything bad in your profile. If you lie about doing something bad, it's a strike against you. If you aren't lying, it's still a strike against you. In some cases students are being expelled from schools for posting threats on these websites. It's serious, and it can affect you for the rest of your life because what you write on the Internet, never is *truly* erased, it ends up going into archives, and even if you try to delete a webpage, it might be indexed on a search engine or an Internet-archive site.



Search on the term Way Back Machine – and you'll find a website that stores and saves the information posted on other websites.

Here's an example of an almost day-by-day copy of what was on the MySpace website in 2005. All of the most popular websites, like Facebook and Black Planet can be searched like this. So if you write something on a community website as a joke and take it down after one day – it still may remain on the Internet forever. So if you search for the term "way back machine" on any search engine – like Google or Yahoo - it will take you to an archive site that records what was on certain websites just like what is on this slide.



There is just so much information! This just means that parents and students have to be educated and agree on what's fair and what's not fair to do on the Internet – because the amount of information on the Internet is almost unlimited. We recommend family discussions. Depending upon what is decided; students will know what is right and fair to do online. If a family decision is reached about parental filtering or tracking, parents can find many different products that provide filtering by conducting an Internet search or talking with someone at a store that sells software. But there is no perfect filtering or tracking solution – every family needs to talk about these issues together and decide what parameters are best for them. **Knowledge is power.** The more you know, the better able you are to make good decisions.



We've have talked about many of the potential dangers inherent when using the Internet.



To conclude our program...here's some very interesting statistics for parents and teens!

<u>For parents</u> - 45% of all 5th graders in an I-Safe study said that if their parents knew everywhere they went online, they would either take their computer away, express concern, or restrict my internet usage.

<u>For teens</u> – if anything or anyone ever bothers or concerns you while you're online, just shut your computer down and talk to your parents or another trusted adult.

For teens and parents – 83% of the people online have admitted to lying to others while being online.

<u>For parents</u> – we recommend you have a family discussion about placing your children's and family computer in an open area – not in anyone's room

 $\underline{For \ teens}$ – your parents should respect your privacy even though you realize that they are responsible for your safety.

For parents -42% of all kids have been cyber bullied online and 35% have been threatened online.

<u>For teens</u> – never agree to meet a stranger that you've meet online and have previously met in person. If you have questions about this – ask your parents. And parents – 12% of all students have said they've meet a stranger they met online "face to face."

<u>For parents and teens</u> – in an I-Safe study, 87% of all adults said that they had made specific rules for their children's Internet use – while only 36% of the students said their parents had – this is a gap of 51% of what parents think and students think!

For parents and teens – in the same study, 69% of the parents said they know a lot about what their children do on the Internet – while 41% of the students say they don't share what they do online with their parents. That's a 28% gap, let alone the 31% of parents that say they don't know a lot about what their children do online!

For everyone – you can find more information by going to safeconnects.org.





And now that you've completed this Safe Connects education program, we hope you know more about each of the topics we've talked about today. And thanks to the Indiana Department of Education for reviewing these slides. However, Net Literacy's Safe Connects is responsible for all of the content.

Remember to have fun and stay safe! Again, if you have ANY questions about Internet safety, visit us at www.SafeConnects.org