Tips for Parents and Teens when Discussing Internet Safety Together with their Family and Friends

In 2006, the first Safe Connects presentations were made by high school students to middle school students and their parents in the schools after school

You have just attended a Safe Connects Internet safety presentation at your school. It was a family event that parents and students attended together. The material that was covered was extensive. Frankly, many feel as if there are almost too many new things that you learned to remember them all!

The Safe Connects program provides you with collateral materials and resources that you can use to further discuss Internet safety together as a family or with your friends. They include:

1. A collection of Public Service Announcements that you may have seen when watching television are available on this site and can be used as a lead in to discuss one of the many important topics. *These have been developed by students but vetted by the IDOE, law enforcement officers, principals, parents, and educators – but Net Literacy is responsible for all of the content.*

2. A 30 minute video is available for you to watch that shows the high school and adult Internet safety presentation. *These have been developed by students but vetted by the IDOE, law enforcement officers, principals, parents, and educators – but Net Literacy is responsible for all of the content.*

3. Three age-appropriate (3rd through 6th grade, middle school, high school and adults) scripted PowerPoint presentations are available for you to read online or download. *These have been*

developed by students but vetted by the IDOE, law enforcement officers, principals, parents, and educators – but Net Literacy is responsible for all of the content.

4. The Resources section includes recommended websites that explain more about Internet safety.

5. This document: Tips for Parents and Teens when Discussing Internet Safety Together withe their Friends and Family – can be reviewed on this page or downloaded by clicking the link on the top of this page.

<u>Please Note:</u> *Net Literacy's student volunteers created this document by identifying what we believed to be the best of class information about Internet safety on the Web, from several authoritative sources. We then modified it to give it our own "plain talking" and "honest" student perspective.*

Some things you should know to help you avoid viruses:

- *Choose and use passwords wisely* – Make certain that your password contains at least 8 characters and includes a variety of numbers, letters, and/or symbols.
- *Download with care*- Download images, applications, and screen savers from trusted sources only. Make certain that you know that the website you are visiting and it is one you can trust.
- *Do not immediately open e-mail attachments*- If you receive an e-mail attachment that you were not expecting (even if it is from someone you know), do not open it—there may be a virus contained within it. Your best bet is to send e-mail back to the sender asking them to explain what the attachment contains. If it is a virus, they may not even know the e-mail was sent. This extra step can really help to protect your system!
- *Avoid forwarding chain letters, jokes, and other types of SPAM*- These letters often contain false information that misleads people. In addition, they send the personal data of yourself and your friends to strangers through malware embedded in the chain-email. By forwarding emails to your friends, you may be creating a list of emails for spammer to use.
- *Be sure to use and update your anti-virus software*- This is your best defense against viruses!
- *Make regular back-ups of your files*- In the case of a virus or computer malfunction, regular back-ups help to get your system back in order quickly.
- *When you receive a message that makes you feel uncomfortable, do not respond*- Immediately shut off your monitor or close your laptop and talk to a parent or trusted adult.
- *Use your computer in a positive manner that is respectful and courteous to others*- Remember, it is important to use your system to do good things—not harm.
- *Protect your personal data by not giving out your name, address, phone number, etc.*- This information should only be given to people that you trust—it's always a good idea to check with your parents before providing this information.
- *Help others to recognize the importance of protecting yourself and your computer system*- Share these steps with your friends and family!

For more information, you can visit the following websites:

- http://www.symantec.com
- http://csrc.nist.gov/virus/
- http://www.howstuffworks.com/virus.htm
- http://www.hoaxbusters.org/
- http://www.faqs.org/faqs/computer-virus/new-users/

Some things you can do to help protect your family from Internet Predators:

- Parents – establish online rules and an agreement with your sons and daughters about Internet use at home and outside of the home.
- Teens – talk to your friends if you see them making poor choices online that could compromise their safety
- Parents – spend time online alongside your daughter or son and establish an atmosphere of trust regarding computer usage and online activities.
- Teens – your parents should respect you, but remember that they have the ultimate responsibility to keep you safe.
- Parents – place your home computer in an area of your house where you can easily supervise your family's Internet activity.
- Parents – regularly discuss your sons and daughters about their online friends and activities. This helps you learn about how the digital generation uses the Internet – and may help keep your family safe.
- Teens -if your brother, sister, or friends seems to be making bad choices online that could harm them, talk with them, and a parent or trusted adult.
- Parents – consider implementing software tools to protect your family from the intrusion of inappropriate content and sexual predators.
- Teens and Parents – block instant/personal messages from people that you or your son and daughter don't know.
- Parents – review the amount of time your son or daughter spends on the Internet, and at what times of day.
- Teens – if a friend "lives" on the Internet – be a friend and invite that person to do something together that's in "the real world."
- Parents and Teens – report any content or activity that you suspect as illegal or criminal to local law enforcement.

For more information on Internet predators, please visit the following web sites:

- http://www.protectkids.com
- http://safety.com

- http://www.crisisconnectioninc.org

Or type “Internet Predators” into your preferred search engine to get the latest developments and news.

From Net Literacy’s student board’s perspective: A Frank Discussion About Cyber-bullying – What’s a Parents’ Role?

Parents need to be the one trusted place youths can go when things go wrong online and offline. Yet they often are the one place kids avoid when things go wrong online. Why? Sometimes, since parents are human, they tend to overreact. The emotion that you express may be a result of the fear you feel or the anger that you have that someone would do something harmful to someone that you love. Sometimes, that’s not the message that comes across. Teens feel as if their parents are yelling at them. In fact, most youths will avoid telling their parents about a cyber-bullying incident fearing they will only make things worse; for example, calling the other parents, the school, blaming the victim or taking away Internet privileges. Unfortunately, some parents also under react, and often don’t get it “just right.”

Parents should be supportive of your son or daughter during this time. You may be tempted to give the “stick and stones may break your bones, but words will never hurt you” lecture, but words and cyber-attacks can wound a youth easily and have a lasting effect. These attacks follow them into your otherwise safe home and wherever they go online. And when dozens of accomplices can be recruited to help target or humiliate your son or daughter online (including some that may have never even met your son or daughter), the risk of emotional pain is very real, and very serious. Don’t brush it off.

Let the school know so the guidance counselor can keep an eye out for in-school bullying and for how your child is handling things. You may want to notify your pediatrician, family counselor or clergy for support if things progress. It is crucial that you are there to provide the necessary support and love. Make them feel secure. Children have committed suicide after having been cyber-bullied, and some young boys and girls have killed other children after a cyber-bullying incident. Take it seriously.

Parents also need to understand that statistically, a teen is just as likely to be a cyber-bully as a victim of cyber bullying. Students sometimes go back and forth between the two roles during one incident. They may not even realize that they are seen as a cyber-bully. Your actions have to escalate as the threat and hurt to your child does. But there are two things you must consider before anything else. Is your child at risk of physical harm or assault? And how are they handling the attacks emotionally?

If there is any indication that personal contact information has been posted online, or any threats are made to your child, you must run; do not walk, to your local law enforcement agency (not the FBI). Take the computer or a printout of all instances of cyber bullying to show them, but note that a printout is not sufficient to prove a case of cyber-harassment or cyber bullying. You’ll need electronic evidence and live data for that. But remember, if in doubt, report it.

Let the law enforcement agency know that the trained cyber-harassment volunteers at WiredSafety.org will work with them (without charge) to help them find the cyber bully offline and to evaluate the case. It is crucial that all electronic evidence is preserved to allow the person to be traced and to take whatever action needs to be taken. The electronic evidence is at risk for being deleted by the Internet service providers unless you reach out and notify them that you need those records preserved. The police or volunteers at WiredSafety.org can advise you how to do that quickly. Using a monitoring product, like Spectorsoft, collects all electronic data necessary to report, investigate and prosecute your case (if necessary). While hopefully you will never need it, the evidence is automatically saved by the software in a form useable by law enforcement when you need it without you having to learn to log or copy header and IP information.

To learn more about Cyber bullying, please visit the following sites:

- http://www.cyberbully.org/
- http://www.cyberbullying.ca/
- http://www.kidscape.org.uk/childrenteens/cyberbullying.shtml
- http://www.isafe.org/
- http://www.bebo.com/CyberBullying.jsp

Some things you can do to help prevent identity theft:

1. Buy a cross-cut type shredder. Shred all your important papers and especially pre-approved credit applications received in your name and other financial information that provides access to your private information. Don't forget to shred your credit card receipts.
2. Be careful of "Dumpster Diving." Make sure that you do not throw anything away that someone could use to become you. Anything with your identifiers must be shredded (cross-cut) before throwing away.
3. Be careful at ATM's and using Phone Cards. "Shoulder Surfers" can get your "Pin Number" and get access to your accounts.
4. Get all of your checks delivered to your bank – not to your home address.
5. Do not put checks in the mail from your home mailbox. Drop them off at a U.S. Mailbox or the U.S. Post Office. Mail theft is common. It's easy to change the name of the recipient on the check with an acid wash.
6. When you order new credit cards in the mail, or your previous ones have expired, watch the calendar to make sure that you get the card within the appropriate time. If it is not received by a certain date, call the credit card grantor immediately and find out if the card was sent. Find out if a change of address was filed if you don't receive the card or a billing statement.
7. Cancel all credit cards that you do not use or have not used in 6 months. Thieves use these very easily – open credit is a prime target.
8. Put passwords on all your accounts and do not use your mother's maiden name. Make up a fictitious word.

9. Get a post office box or a locked mailbox, if you possibly can.
10. Ask all financial institutions, doctors' offices, etc., what they do with your private information and make sure that they shred it and protect your information. Tell them why.
11. Memorize social security numbers and passwords.
12. When a person calls you at home or at work, and you do not know this person, never give out any of your personal information. If they tell you they are a credit grantor of yours call them back at the number that you know is the true number, and ask for that party to discuss personal information. Provide only information that you believe is absolutely necessary.
13. Do not put your telephone number on your checks. Do not put your credit card account number on the Internet (unless it is encrypted on a secured site.)
14. Don't put account numbers on the outside of envelopes, or on your checks.
15. When you are asked to identify yourself at schools, employers, or any other kind of institutional identification, ask to have an alternative to your social security number. Unfortunately, your health insurance carrier often uses your social security number as your identification number. Try to change that if you can.
16. In conjunction with a credit card sale do not put your address, telephone number, or driver's license number on the statement.
17. Monitor all your bank statements from every credit card every month. Check to see if there is anything that you do not recognize and call the credit grantor to verify that it is truly yours.
18. Order your credit report at least twice a year (I have enclosed the addresses for you on the sample letter.) Review it carefully. If you see anything that appears fraudulent, immediately put a fraud alert on your reports by calling the numbers below.
19. Immediately correct all mistakes on your credit reports in writing. Send those letters Return Receipt Requested, and identify the problems item by item with a copy of the credit report back to the credit reporting agency. You should hear from them within 30 days.
20. Write to your State and Federal Legislators to demand stronger privacy protection. Also, ask that identity theft be considered a crime in your State. Demand that the State Finance and Banking Committees pass legislation to protect consumers from negligent bank and credit reporting practices.
21. Consider making your phone an unlisted number or just use an initial for your first name.
22. Make a list of all your credit card account numbers and bank account numbers (or photocopy) with customer service phone numbers, and keep it in a safe place. (Do not keep it on the hard drive of your computer if you are connected to the Internet.)
23. Take your name off all promotional lists. Call the three credit reporting agency numbers to opt out of pre-approved offers. –>Take your name off all promotional lists. Call the three credit reporting agency numbers to opt out of pre-approved offers for Experian, Equifax, and TransUnion – call 888-567-8688 – call one number and remove yourself from the promotional lists maintained by the three major credit reporting agencies.

Write to the following to get off promotional lists:

Direct Marketing Association Mail Preference Service P. O. Box 9008 Farmingdale, NY 11735	Direct Marketing Association Telephone Preference Service P. O. Box 9014 Farmingdale, NY 11735

(Retrieved from: http://www.identitytheft.org/ – with some modifications by Net Literacy student volunteers)

Here are a few other websites that address identity theft:

- **http://www.consumer.gov/idtheft/**
- **http://www.privacyrights.org/identity.htm**
- **http://www.usdoj.gov/criminal/fraud/idtheft.html**
- **http://www.idtheftcenter.org/**
- **http://www.identitytheft.org/**

Things to consider when creating a profile:

- **A profile is a personal page about you and what you like.**
- **Profiles basically contain four things; name, age, gender and location.**
- **You can make a profile on various community web sites, chat rooms, emails, and instant messaging.**
- **Only include non-important things in a profile; nothing personal or valuable.**
- **Something to consider when profiling; you should include the input from a parent when creating a profile.**

Ways to break the chain:

- **If you see a chain letter, click the X in your right hand corner (in other words – close the document and then delete it).**
- **Don't send the chain letter to anyone else**

Ways to protect yourself from archive websites:

- **Watch what you put on the internet**
- **Watch who you associate with online.**

On the Internet, don't count on anything ever being erased. Google "The Way Back Machine" or visit http://www.archieves.org and you see that websites that have been saved from the 1990s. You cannot count on something that is written ever being completely erased – someone with enough skill can often find almost anything. Is this intrusive, and unnerving? The students at Net Literacy think so – and that's why we created an Internet safety PSA explaining "that what you say may be used against you, forever."

Ways to keep safe in chat rooms:

- **Do not give out phone numbers or address on line even if you think you might know them**
- **Do not use all caps in one word (SHUT UP)**
- **If you feel threaten the leave and tell a parent or a trusted adult immediately.**

For more safety tips, you can go to the following websites:

- **http://www.safekids.com/**
- **http://yahooligans.yahoo.com/parents/**
- **http://www.staysafe.org/**
- **http://www.wiredwithwisdom.org/**
- **http://www.wiredsafety.org/**
- **http://www.surfnetkids.com/**
- **http://www.thinkuknow.co.uk/**
- **http://www.bewebaware.ca/english/default.aspx**
- **http://www.childnet-int.org/projects/**
- **http://www.cyberpatrol.com/**

Net Literacy's student volunteers created this document by identifying what we believed to be the best of class information about Internet safety on the Web, from several sources. We then modified it to give it our own "plain talking" and "honest" student perspective.

Please email any questions to danielkent@netliteracy.org