

INTERNET SAFETY TIPS FOR FAMILIES (ELEMENTARY SCHOOL)

The Internet offers a world of resources and poses a variety of dangers for our youth, such as: viruses that could harm your computer; pedophiles that are trying to meet your child; disclosing personal information that could lead to identity theft; and cyber-bullying. Every parent must recognize these dangers to help their child learn to protect his/her self-online. The following are some safety tips for parents of elementary students who use the Internet.

SAFETY TIPS

Since you may not always be able to watch everything your child does on the computer, most experts recommend installing monitoring software to ensure that you know exactly what your children are doing online.

Place the computer in a common area. It is suggested that your child not have computer in his or her room, or at least no Internet access.

Learn to use the Internet yourself. Experience cyberspace with your child and learn how to check the computer's "History" to see what websites your child is visiting.

Tips for youth to stop cyber-bullying:

- Don't initiate, respond or forward harmful messages.
- Think first! If something mean is posted or texted about you, don't respond immediately. Take a break and give yourself time to think through your next step.
- Think about your reputation--would you want your grandma, teacher, future employer, or someone you don't know, to see your post?
- Trust your gut. If you feel uncomfortable, save the message, and tell an adult.

Tips for parents regarding cyber-bullying:

- Ask your children questions. Maintain an open dialogue.
- Keep the computer in a common room.
- Talk about your expectations regarding acceptable online/phone behavior before they receive the privilege. Behavior online should be the same as what you would do in person or in front of someone you respect.
- Make agreements and set boundaries about accepted use and behavior for online/phone communication. Often youth don't tell parents because they fear losing their technology privileges.
- Help your child think through how the information they put online reflects on them.
- Inform youth about legal and future consequences of harmful posing online or by phone.
- Ask your child to teach you about programs or technologies you don't understand or of which you don't have familiarity.
- Model the behaviors you want to see around phone and internet use.

Key Messages

- Spend time with your child on the Internet to demonstrate to his/her proper use.
- Monitor your child's computer use and Internet "History."
- Establish rules for your child's Internet use.
- Never give personal information to someone you do not know.
- Report any suspected cyber child sexual exploitation to the NCMEC CyberTipline.
- Be careful of any information you post online, including photos, which will be available for anyone to view, forever.
- Beware of cyber predators!

Talk to your child about the dangers online.

Your child should know that:

- Accepting files or downloads from unknown sources can bring a virus that could harm the computer.
- Giving away personal information can lead to identity theft or worse.
- People may not be who they say they are online. (Predators roam cyberspace.)
- It is important to keep passwords private.
- Open communication with your child is vital. Your child needs to feel they can come to you if they encounter frightening communications or images without fear of losing Internet privileges.

If you have a webcam, your child should use it ONLY if you are present. Posting pictures online or sending images can have dangerous consequences. Parents *must* control such activity.

Note to Parents: There are many organizations and activities in which your child may be involved that post information online in public locations. It is extremely important for you to pre-approve any information about your child that will be posted for the world to see. Remember, cyber predators are looking too.

TEACH YOUR CHILDREN THE FOLLOWING RULES:

- ✓ **Never accept files or downloads from unknown sources. This includes familiar sources if you were not expecting them.**
- ✓ **Choose an email address/ screen name that DOES NOT contain any part of your name, age, gender, interests, or favorite activities.**
- ✓ **Do NOT fill out a profile without parent review and approval.**
- ✓ **NEVER give out real name, telephone or cell phone number(s), mailing address, or passwords.**
- ✓ **Do NOT enter chat rooms.**
- ✓ **Do NOT post photographs in publicly accessible sites.**
- ✓ **The settings for ANY social networking profiles* should be PRIVATE, and new friends are accepted only if they are known to the child AND parent.**

**Social networking sites include Facebook, Twitter, Instagram, Snapchat, etc.*

INTERNET SAFETY TIPS FOR FAMILIES (MIDDLE SCHOOL)

SAFETY TIPS

Since you may not always be able to watch everything your child does on the computer, most experts recommend installing monitoring software to ensure that you know exactly what your children are doing online.

Place the computer in a common area. It is suggested that your child not have computer in his or her room, or at least no Internet access.

Learn to use the Internet yourself. Experience cyberspace with your child and learn how to check the computer's "History" to see what websites your child is visiting.

If you have a profile on a social networking site*:

- Set up profile to **Private** or **Friends Only** – otherwise private information can be spread very quickly to known and unknown people.
- Only add people to your friends list that you already know.
- Protect your personal information as well as personal information about your friends.
- If you are too young to be on a site, don't lie about your age to join.
- Delete mean or embarrassing comments.
- Beware of invitations through comments or bulletins to view videos or click on links. They may be attempts to capture your password and introduce a virus.

Tips for youth to stop cyber-bullying:

- Don't initiate, respond or forward harmful messages
- Think first! If something mean is posted or texted about you, don't respond immediately.
- Take a break and give yourself time to think through your next step.
- Think about your reputation--would you want your grandma, teacher, future employer, or someone you don't know, to see your post?
- Trust your gut. If you feel uncomfortable, save the message and tell an adult.

Tips for parents regarding cyber-bullying:

- Ask your children questions. Maintain an open dialogue.
- Keep the computer in a common room.
- Talk about your expectations regarding acceptable online/phone behavior before they receive the privilege. Behavior online should be the same as what you would do in person or in front of someone you respect.
- Make agreements and set boundaries about accepted use and behavior for online/phone communication. Often youth don't tell parents because they fear losing their technology privileges.
- Help your child think through how the information they put online reflects on them.

Key Messages

- Spend time with your child on the Internet to demonstrate to his/her proper use.
- Monitor your child's computer use and Internet "History."
- Establish rules for your child's Internet use.
- Never give personal information to someone you do not know.
- Report any suspected cyber child sexual exploitation to the NCMEC CyberTipline.
- Be careful of any information you post online, including photos, which will be available for anyone to view, forever.
- Beware of cyber predators!

- Inform youth about legal and future consequences of harmful posing online or by phone.
- Ask your child to teach you about programs or technologies you don't understand or of which you don't have familiarity.
- Model the behaviors you want to see around phone and internet use.

Remember that anyone can lie online. A stranger could be a cyber predator if:

- The stranger asks for your picture.
- The stranger invites you to view their web cam.
- The stranger asks if you are alone.
- The stranger talks about sexual matters.
- The stranger wants to meet you in person.

If you are thinking about posting your pictures on a public site, think about this:

- Once you have placed your picture on a public Internet site, it's out there forever and there is no taking it back.
- Software manipulation of photographs makes it possible for that photo to be altered and put back on the Internet or traded among child pornographers.
- Be anonymous: Don't give away personal information in your username or screen name. Don't use passwords that are easy to guess (i.e., the name of your pet).

Is Your Computer Protected?

- **What do you do with email from unknown sources?** Opening an email from an unknown source, particularly if there is an attachment, may introduce a virus that could permanently damage your computer.
- **Do you post your email on public sites?** Spammers can find your email on the Internet and use it send you junk email.
- **Does it have anti-virus software installed?** Protect your files and computer from virus attacks that can prove disastrous.
- **Do you have a firewall?** One of the best ways to protect your computer from the ravages of hackers is to install a firewall.
- **Do you know the dangers of file sharing?** Someone could infect your computer with a virus or access information from your hard drive. This could be particularly devastating if financial information is stored on the computer.
- **Do you forward emails from unknown sources?** You may think you are being helpful, but by forwarding the email, but you have just provided your friend's email address to an unknown source. And, if there is an attachment, you may have forwarded a virus.
- **Do you disconnect the Internet when it's not in use?** This is the best way to prevent anyone from using the Internet's "two-way street" to get into your computer.

**Social networking sites include: Facebook, Twitter, Instagram, Snapchat, etc.*

INTERNET SAFETY TIPS FOR FAMILIES (HIGH SCHOOL)

Tips for youth to stop cyber-bullying:

- Don't initiate, respond or forward harmful messages
- Think first! If something mean is posted or texted about you, don't respond immediately. Take a break and give yourself time to think through your next step.
- Think about your reputation--would you want your grandma, teacher, future employer, or someone you don't know, to see your post?
- Trust your gut. If you feel uncomfortable- save the message and tell an adult.

Tips for parents regarding cyber-bullying:

- Ask your children questions. Maintain an open dialogue.
- Keep the computer in a common room.
- Talk about your expectations regarding acceptable online/phone behavior before they receive the privilege. Behavior online should be the same as what you would do in person or in front of someone you respect.
- Make agreements and set boundaries about accepted use and behavior for online/phone communication. Often youth don't tell parents because they fear losing their technology privileges.
- Help your child think through how the information they put online reflects on them.
- Inform youth about legal and future consequences of harmful posing online or by phone.
- Ask your child to teach you about programs or technologies you don't understand or of which you don't have familiarity.
- Model the behaviors you want to see around phone and internet use.

Tempted to meet someone face-to-face that you know only from online chats?

Remember anyone can pretend to be anyone online. A skilled predator will pretend to be exactly the type of person you are looking for; otherwise, you wouldn't be interested in getting together, would you? If you think you can't meet a predator, think again. Predators go anywhere you go on the Internet.

Sharing too much information about yourself?

Would you walk around with private information taped on your back, so anyone could read it? Probably not, however, this is what you are doing when you post private information on social networking sites and don't have your privacy settings set to PRIVATE or FRIENDS ONLY. You, your friends, and your athletic teams are putting information about you onto the web. If the world can see that information, so can a predator or a stalker. Guard your personal information and ask others to be careful with it as well.

There is another potential problem that you might not consider – *identity theft*. This is a crime in which someone establishes credit in your name. Unfortunately for you, the credit history that is established will

Key Messages

- Spend time with your child on the Internet to demonstrate to his/her proper use.
- Monitor your child's computer use and Internet "History."
- Establish rules for your child's Internet use.
- Never give personal information to someone you do not know.
- Report any suspected cyber child sexual exploitation to the NCMEC CyberTipline.
- Be careful of any information you post online, including photos, which will be available for anyone to view, forever.
- Beware of cyber predators!

not be a good one, and it will take a lot of time and effort to clean up the mess. Giving out personal information should be *your* decision. Just because an interesting website asks for your personal information doesn't mean you should give it out.

Be careful posting photos of yourself on the web. Photos placed on public sites can be manipulated and placed back on public sites. Such photos of you might prove to be embarrassing or worse – not the kind of photo you would want a college admissions committee or potential employer to see.

What do you know about intellectual properties?

Do you know that intellectual properties are protected by copyright law? And using another's intellectual properties without their permission is illegal.

Many owners of intellectual properties view piracy and plagiarism as stealing. Illegal downloading of movies and music can have serious legal and monetary consequences. The music industry has taken legal action against some offenders, typically costing the person thousands of dollars to resolve.

Plagiarizing can seriously damage your academic record which could adversely affect college admission or getting a job.

EXAMPLES OF INTELLECTUAL PROPERTIES

- Music Recordings
- Videos
- Photographs
- Drawings
- Magazine Articles
- Computer Games
- Computer Software
- Books

INTERNET SAFETY TIPS FOR PARENTS (ALL LEVELS)

SOME ONLINE BEHAVIORS ARE AGAINST THE LAW...

Many view piracy and plagiarism as stealing. Illegal downloading of movies and music can have serious consequences. Just as stealing a CD or DVD from a store is wrong, so is stealing online.

There is an area of the law called Intellectual Properties. Learn about it. Copying information from the Internet can be illegal and there are risks.

PROTECTING YOUR COMPUTER

Emails from unknown sources may contain attachments that introduce viruses that permanently damage your computer. Forwarding emails from unknown sources can reveal your friend's email address to the sender and possibly infect your friend's computer with a virus.

File sharing can lead to a virus or provide access to information contained on your hard drive.

Installing a firewall can help protect your computer from the problems created by hackers.

Anti-Virus software can help protect your files.

Disconnecting your Internet when not in use is the best way to prevent anyone from using the Internet's "two-way street" to get into your computer.

Posting your email address on public sites allows spammers to find it and send you junk mail.

REMEMBER: YOUR FIRST AND BEST LINE OF DEFENSE IS SELF-DEFENSE IN CYBERSPACE.

Note to Parents: There are many organizations and activities in which your child may be involved that post information online in public locations. It is extremely important for you to pre-approve any information about your child that will be posted for the world to see. Remember, cyber predators are looking, too.

IF YOU SUSPECT THAT YOUR CHILD HAS BEEN CONTACTED BY A PREDATOR

Notify law enforcement

OR

File a complaint online at www.missingkids.com

Reporting Child Sexual Exploitation: If an incident occurs in which you feel your child is a victim of online solicitation for sexual acts, sextortion, or child pornography, PLEASE report the incident to the National Center for Missing & Exploited Children® (NCMEC). Their website is www.missingkids.org.

The NCMEC's CyberTipline is operated in partnership with the FBI, Immigration and Customs Enforcement, U.S. Postal Inspection Service, U.S. Secret Service, military criminal investigative organizations, U.S. Department of Justice, Internet Crimes Against Children Task Force program, as well as other state and local law enforcement agencies. Reports to the CyberTipline are made by the public and Electronic Service Providers (ESP). ESPs are required by law to report apparent child pornography to law enforcement via the CyberTipline (18 U.S.C. § 2258A).

Reports are continuously triaged to help ensure that children in imminent danger get priority. Analysts review reports and:

- Examine and evaluate the content.
- Add related information that may be useful to law enforcement.
- Use publicly available search tools to determine the geographic location of the apparent criminal act.
- Provide all information to the appropriate law enforcement agency for potential investigation.

The CyberTipline reporting mechanism assists law enforcement and prosecutors in their detection, investigation, and prosecution of child sexual exploitation crimes. The CyberTipline helps make law enforcement's efforts more efficient and maximizes the limited resources available in the fight against child sexual exploitation. The value of the CyberTipline as a source of leads for law enforcement has been greatly enhanced by collaboration with ESPs.

In addition to referring CyberTipline reports to law enforcement for potential investigation, the NCMEC engages with the Internet industry on voluntary initiatives to reduce child sexual exploitation online.