U.S. Department of Justice

United States Attorney
District of Maryland

Vincent DeVivo
Community Outreach Specialist
Vincent.Devivo@usdoj.gov

Suite 400
36 S. Charles Street
Baltimore, MD 21201-3119

DIRECT: 410-209-4832
CELL: 240-460-1374
FAX: 410-962-9293

February 1, 2017

Dear Lake Elkhorn Middle School Community Member:

Parents, teachers and community organizations play a critical role in securing the safety and welfare of children, and the United States Attorney's Office is eager to partner with you in promoting a safe and healthy learning environment in your community.

Innocence Stolen: Protecting Our Children Online is a multimedia presentation that provides communities the necessary information to keep children safe on the internet. This internet safety program is free of charge and available for your community, PTA, school faculty, and professional development meetings throughout the school year.

The presentation informs adults about how best to protect young people from negative and criminal influences online. Topics include social networking, cyber bullying, sexting, and internet predators. The program provides prevention and intervention strategies and internet safety resources.

Please contact me for more information and scheduling.

Vince DeVivo
Community Outreach Specialist
United States Attorney's Office, District of Maryland
36 S. Charles Street, Fourth Floor
Baltimore Maryland 21201
Office: 410-209-4832
Cell: 240-460-1374
Vincent.Devivo@usdoj.gov

Internet Golden Rules

1. Rules from "real" life apply: courtesy, kindness, modesty, dignity, respect for the law and others, etc.
2. Don't talk to strangers.
3. Keep your private information private.
4. Never agree to meet an online friend without your parents.
5. There are no guarantees that what you say or post on the Internet is private.
6. Information, including photos, videos, etc., posted on the Internet can last forever.
7. Watch for apps that are difficult to understand, have a hidden purpose, or access your camera.
8. Find the "good" online – good friends, good Web sites, good games – and enjoy.

Internet, Mobile Phones, and Texting Safety Tips

Parents

- Do teach your child not to post identifying information on the Internet.
- Do set a limit for how much time your child can spend online.
- Do keep the computer in a public room in the house. Do not have an Internet-connected computer in your child's bedroom.
- Do utilize parental controls provided by your Internet Service Provider and/or blocking software. (Contact your Internet ISP if you have questions).
- Do talk to your children about purchasing "in app" products.
- Do talk to your child about using any location services on their device.
- Do periodically review your child's computer, emails and messages. You should have all of your children's passwords.
- Do spend time with your child online. Have them show you their favorite online destinations. Get to know your child's online friends as you would their real-life friends. Learn to navigate the web.
- Do know who they text and email. Most providers have online ways to identify frequent contacts so you can see if someone new appears as a contact.
- Do monitor your child's access to the Internet and texting.
- Do talk to your child about the danger of Internet predators.
- Do watch for unexplained changes in your child's behavior.
- Do NOT hesitate to seek help from law enforcement if you think a predator may be targeting your child.

For more helpful Internet safety information, please visit www.netsmartz.org. Netsmartz.org has age appropriate videos, activities, and information for students in elementary school, middle school, and high school.

Internet, Mobile Phones, and Texting Safety Tips

Students

- Do not post personal information online (name, age, birth date, address, telephone number, or school name). This information can be used by others to find out where you and your family live.
- Do not post your picture or pictures of your family online – they can be copied or changed or used to find you.
- Do not send any inappropriate photo or message by email or text.
- Do not post your plans and activities in a chat room or on your personal website. Do not post entries that make it clear that no one is at your home.
- Do not communicate with someone who has made you uncomfortable or afraid. Tell your parents or a trusted adult if someone does.
- Do not join online groups or games without talking to your parents.
- Do not meet with someone you met online without first telling your parents or guardian.
- Do not post hurtful or inappropriate messages. If someone else posts hurtful or inappropriate messages -- do not respond, but do tell a teacher, parent or other adult.
- Do not click on any link that you do not know, and you are not sure is legitimate.
- Do not buy any "apps" or "in app" purchases without talking to your parents or guardian.
- Do not enable any location services without talking to your parents or guardian.
- Do remember that people can lie online and say they are something they are not. Someone who says they are a 12-year-old girl could really be an older man looking to harm you.
- Do save messages that upset you and show them to your parents.
- Do share your password with your parents.
- Do visit www.netsmartz.org to learn more about Internet safety.

Filters, Controls, and Access Restrictions*

Apple iPhone, iPad, and iPod- Restrictions

Restriction settings allow you to restrict access to apps and features, filter content, and prevent changes you set to privacy settings. This will require a passcode, one that is separate from the lock screen pass code.

https://support.apple.com/en-us/HT201304

Apple Ask to Buy:

Works in family sharing mode. Prohibits downloads from the App Store without parent approval. Child purchase requests are sent to parents for approval. If approved, the app will automatically download.

https://support.apple.com/en-us/HT201089

Android Parental Control Features:

Android devices use a combination of apps and restricted profiles to allow for restricting access to apps and content. Apps can be found in Google Play.

http://www.pcadvisor.co.uk/how-to/google-android/3461359/parental-control-on-android/

Verizon Specific Tools:

Tool/Utility	Description	Cost	Link
Safeguards	General information on the types of utilities are available	N/A	**https://my.verizonwireless.com/vzw/nos/safeguards/safeguardLandingPage.action**
Content Filters	Filter content based on movie type ratings:	Free	**https://my.verizonwireless.com/vzw/nos/safeguards/SafeguardProductDetails.action?productName=contentfilters**
FamilyBase	With this utility you can view all app purchases and see which ones are used the most. You can restrict access to apps, times of use, and monitor activity.	$4.99 / month	**https://my.verizonwireless.com/vzw/nos/safeguards/SafeguardProductDetails.action?productName=familybase**
Service Block	Block certain services from your mobile device.	Free	**https://my.verizonwireless.com/vzw/nos/safeguards/SafeguardProductDetails.action?productName=serviceblock**

AT&T Wireless:

Tool/Utility	Description	Cost	Link
Smart Limits	Set limits on usage, block phone numbers, and keep tabs on calls and texts.	$4.99 / month 1-line; $9.99 / month for up to 10	**https://smartlimits.att.com/#/**

T-Mobile Wireless:

Tool/Utility	Description	Cost	Link
WebGuard	Blocks or filters web page content.	Free	**https://support.t-mobile.com/docs/DOC-2144**

*This is not an exhaustive list of settings, services, or techniques that can be used to protect your children. Contact your internet and/or cellular provider or use your favorite search engine to learn more.

--information compiled and provided by Chris Salmi, a concerned parent

Talking with Kids About the Internet

- How much does it cost to join Facebook, Instagram, or other social media site?
- What do you consider to be inappropriate material on the internet?
- Have you ever come across inappropriate content on the internet? What did you do?
- What would you do if you came across a pop-up of a naked person or hateful speech against a person or group?
- Would you feel comfortable telling me about anything you saw online that made you feel scared or uncomfortable? Why or why not?