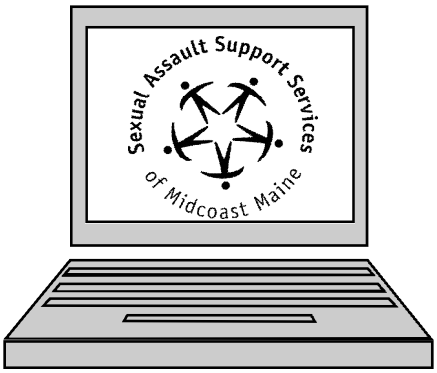

Project Internet: Exploration and Safety

Internet Safety Tip Sheet

Acronyms and Definitions:

AIM- America Online Instant Messenger

Blog- A type of online journal comprised of links and postings.

IM- Instant Message/Messaging.

ISP- Internet Service Provider

SNS- Social Networking Site

URL- Uniform Resource Locator. It is a reference or address to a resource on the Internet.

Identifying Suspicious Emails and/or Phishing links:

- If an email offer sounds too good to be true, it probably is. You can't win a lottery if you don't buy a ticket and you should never give a stranger money, even if they promise that you'll get it back plus more.
- In a website link, always look for the first "/" after the "http://". The words that come directly before it will tell you who "owns" that website.
- URLs with all numbers at the beginning are usually a scam.
- If you aren't sure about a link that claims to be from your financial institution, go to their official website and login from there.
- Most online banking companies now have a section on their website for phishing and how to report suspicious emails. You can forward the message to the institution's technical support if you think it is suspicious.

Tips to Avoid Identity Theft:
*From the Maine Department of Professional and Financial Regulation

- Know what's in your wallet. Don't carry your Social Security number with you and carry only the cards you need every day.
- Shred anything with personal information on it before trashing, including statements and pre-approved offers.
- Never give out personal information to solicitors, whether online, in person or on the phone, even if an email asks you to "verify" your private information.
- Monitor your credit accounts and credit score for unfamiliar activity.
- Address any unauthorized actions immediately.

SASSMM, P.O. Box 990, Brunswick, ME 04011, Office: 207-725-2181, Hotline: 1-800-822-5999

United Way

Funding for this project is provided through the Verizon Foundation.

Internet Respect Plan/Internet Safety Guidelines:

- Develop a household Internet Respect Plan or a set of guidelines. There are two samples included* in your packet.
- Post the plan in the computer area, so the guidelines are visible.
- Work with children to develop the plan. Different ages may need different guidelines to meet their needs.

Social Networking Site Safety:
*Adapted From the MySpace.com Parents Guide

- Don't forget that SNS profiles and forums are public spaces. Don't post anything you wouldn't want the world to know (such as your last name, phone number, home address, IM screen names, or specific whereabouts). Avoid posting anything that would make it easy for a stranger to find you, such as where you hang out every day after school or your school name and mascot.
- People aren't always who they say they are. Be careful about adding strangers to your friends list. Be careful of adding your friends' friends to your own list. Do not meet people in person that you meet online. If you must meet someone, do it in a public place and bring a friend or trusted adult.
- Harassment, hate speech and inappropriate content should be reported. If you feel someone's behavior is inappropriate, react. Talk with a trusted adult, or report it to the SNS or the authorities.
- Don't post anything that would embarrass you later. Think twice before posting a photo or information that you wouldn't want a potential college recruiter, boss or teacher to see!
- Don't lie about your age. Social networking sites protect their users of varying ages. When you lie about your age you circumvent these safety measures and many SNS must take action on your profile upon discovering the misrepresentation. Additionally, do not try and access content or areas that are inappropriate for your age group.
- Decide if it is appropriate for you and/or your child to have a page on a social networking site. Ask your child to teach you how to set up a profile on a social networking site. Ask them to show you theirs regularly and explain why.

Red Flags that a child might become a victim:

- The child becomes withdrawn from family or friends, isolates him/herself more often.
- He/She is spending more time online or is spending much less time online.
- He/She turns off the computer screen or minimizes windows when you walk in the room.
- You find pornography on the computer.
- Your phone bill has calls to unknown numbers.
- The child receives mail/gifts/packages from senders you don't know.

SASSMM, P.O. Box 990, Brunswick, ME 04011, Office: 207-725-2181, Hotline: 1-800-822-5999

Funding for this project is provided through the Verizon Foundation.