Internet Safety Pre-Assessment

- Take the Internet Safety Pre-Assessment
- Let's see how much you know. Take a few minutes and answer the 6 question on the first page of your notes
- When done answer the next three questions on your notes, you may brain storm with your neighbors:
  - What is good about the Internet? Bad?
  - Answer questions 1-5
- Stop at "Disguises"

Objectives

- Students will be able to:
  - Identify dangers of the Internet and discuss ways to stay safe
  - Compare and contrast his/her before and after beliefs on Internet safety
  - Work as a group to create a list of Internet dangers/crimes
  - Identify how to protect themselves from inappropriate Internet behavior

ITF Competencies

- 6670.20 Demonstrate an understanding of Internet use and security issues.
- 6670.41 Examine social, ethical, and legal issues associated with information technology.

Internet Safety

Mrs. Robison

IT Fundamentals

Disguises

- Going on the Internet is like going out on Halloween
  - Everyone's identity is hidden
  - Unless you know your friends' costume, you DON'T know who you're talking to.
  - Any stranger can pretend to be a friend and you have no way of knowing who they are.

Internet Safety

Appropriate Websites

- Feel embarrassed or uncomfortable with what you see – tell an adult

Appropriate Email and Messages

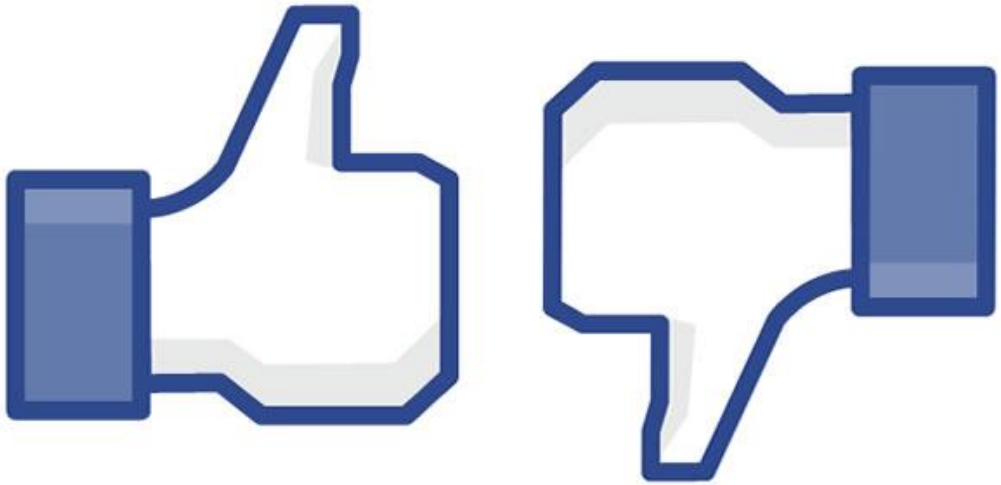
- Do not open email from strangers
- Do not open email with attachments
- Do not give out your email address
- Do not open links or files from people you don't know
- Never respond to e-mails with pornographic or other inappropriate material
- Do not respond to advertisements – this confirms that you have a working e-mail account, and you will only receive more junk e-mails

Giving Out Information

- DO NOT GIVE OUT PERSONAL INFORMATION
  - Name
  - Where you live-city or address
  - Telephone Number
  - Birth date
  - Height
  - Weight
  - Photo
  - Parent's name
  - School

INFORMATION YOU CAN GIVE OUT

- Likes and dislikes



Can you answer these questions?

- Can you tell someone you like blue? ✓
- You like pizza? ✓
- Type of pets that you have? ✓
- Your favorite movie? ✓
- Your favorite movie theater? ✗
- Your favorite beach? ✗
- Teacher's names? ✗

Online names (User Name)

- Be careful of online names – don't give TMI in name
  - Sunygirl14
  - Sweetie15
  - Goldguy17
  - 90tampa

NetSmartz Workshop
A PROGRAM OF THE NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN

PROFILE PICTURE
Is there anything about your picture that could get you in trouble, like nudity, alcohol, or drugs? Remember, this picture will be public!

ACCOUNT/SETTINGS
This is where you'll adjust your privacy settings. Go through each option slowly. Always ask yourself – *what* is on my profile and *who* can see it?

INFORMATION/ ABOUT ME
What are you sharing about yourself? Delete anything that could be too much information, like where you live or go to school. You don't have to fill in every empty box!

USERNAME
This is either your real name or a nickname. Using a real name isn't bad; it just means you have to look more closely at your privacy settings and contacts.

COMMENTS/WALL
Delete any inappropriate comments, and don't forget to be careful what you post on others' pages, too.

FRIENDS/CONTACTS
This list may include people you only know online. Go through each friend and decide if you want to give them access to your page. Why do they *really* want to be your friend?

ADS/APPS
If you click on these or add them to your profile, you're allowing companies access to your personal information. Always read the fine print and decide what's OK to add and what's not.

PHOTOS/ALBUMS
What kinds of photos are you sharing? *Who* can see them? Don't post anything you could get in trouble for, like nudity, alcohol, or drugs.

Mailing list

- Be careful in joining mailing lists, some may make your personal information public.
  - Newsgroups, forums, and bulletin boards – remember not to slip and say anything that can reveal your identity age (little pieces of info can be put together over time)
  - You give out your school colors, and two conversations ago you said you were from a town by Seattle, and in another conversation you said the school mascot was the hawk – and you've just told someone where you are.

Information you provide

- Profiles – be sure they do not reveal your town, name, school
- Website – if you build a website – do not put any specific information on it (even code that isn't displayed can be read by anyone) Do not register it with your name.

Meeting People

- If someone asks to meet you – tell an adult immediately
- Chat rooms are particularly dangerous – people you meet in chat rooms can easily be adult “predators” with misleading names such as “jason15” “cutiepie08”
- Never arrange a face-to-face meeting with someone you meet online (you have no way of really knowing if that person is a 15 year old boy – or a 50 year old man)

Passwords

- Your personal password is your own special identity, so keep it secret and only share it with a parent or guardian (change it often).

How many characters are in your password?

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

1x2x3x4x5x6x7x8x9x10x11x12x13x14x15x16 = 20,922,789,890,000

Managing your Password Activity

How Strong is your password?

Scenarios

- Cindy has been talking online to a girl named Julie for a few days now. Julie has told Cindy where she lives, how old she is, where she goes to school, and what she looks like. Julie asks Cindy what school she goes to. Is it okay for Cindy to tell her?

- Michael is online talking to his friend from school, Chris. They are working on their homework together and studying for a test. Chris says they should meet before class to review for the test. Is this okay?

- Jennifer is talking to a friend online when she gets a message saying there is trouble with her computer and she needs to type in her online password again. Should she do it?

- Jake is talking to a friend online who he met on the Internet. The friend offers to help him finish his homework and asks for Jake's phone number. Is it okay for Jake to give it to him, since it has to do with homework?

- Allison met Linda on the Internet and has been talking to Linda online for several months. Linda says she is the same age as Allison and lives nearby. Linda wants to meet Allison in the mall to go shopping. Should Allison go meet her?

- Jeff got an e-mail from someone he doesn’t know, with a file attached. Should he open it?

- Tina gets an online message from a woman who says her name is Mrs. Anderson and tells Tina that she is a math teacher. Mrs. Anderson wants to know what school Tina goes to and what her teacher's name is. Should Tina tell her?

- Paul is online when he gets a message saying he won a free Xbox! He just needs to send in his address and phone number so it can be mailed to him. Should he give the information?

Tell someone

- Adults get tricked all the time too. Don't be afraid to tell your parents, they will know what to do or at least who to ask.

Complete

- Take a few minutes and to complete “Managing Passwords”
- Read Internet Safety Safeguarding your stuff Your online image “Get the Facts”

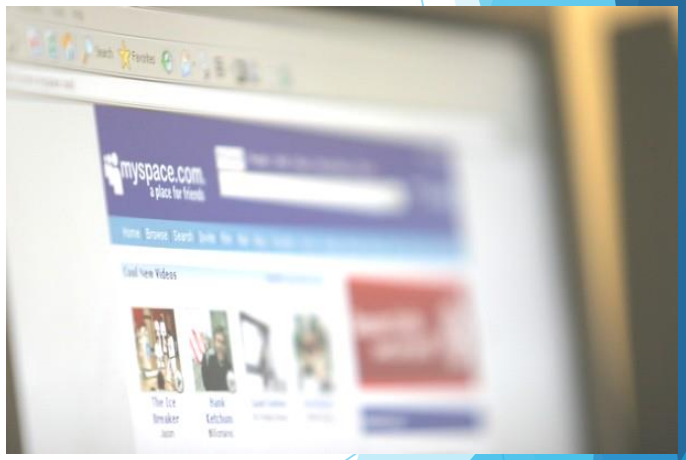
VA State Laws Relating to the Internet

The presentation was created by:
A Deputy
Stafford County Sheriff's Office
Modifications made to formatting and
relevance to the lesson

Internet Safety

Lesson Focus:

- Virginia laws designed to protect internet users;
- Hazards on the internet
- What cyber bullying is?
- Sexting
- Strategies for safe internet surfing.



Laws specifically intended to help protect you online

These laws address:

- Computer Use
- SPAM
- Computer Trespass
- **Harassment using a computer**
- **Threats of death or Bodily Injury**

Computer Use

- Code of Virginia 22.1-70.2 addresses internet use policies for public and private schools
- Amended 2006 in which Virginia became the 1st state in the nation to require internet safety to be integrated into all instructional programs
- You are required to agree to rules established by King George County Public Schools in order to use the school computers and computer network
- ACCEPTABLE USE AGREEMENT (student signature sheet)

King George County School Code of Conduct Rule #8

Computer violations including trespass, fraud, invasion of privacy, and theft of services; unauthorized use of school computer and/or computer network; removal of computer data, programs, software; intentionally causing a computer and/or computer network to malfunction; use or duplication of software in violation of law or licensing requirements; unauthorized access to any portion of a computer network, restricted programs and/or computer drives; unauthorized use of assigned computer passwords to gain access to computer and/or network; any unauthorized use of a school computer code(s); failure to abide by acceptable use agreement.

KGCS Acceptable Use Policy

Computer Crimes

18.2-152.4 - Prohibits Computer Trespass

18.2-152.3:1- Prohibits SPAM, unsolicited bulk email or junk mail

These laws address:

- Spam, junk mail, computer trespass
- Invasion of privacy using a computer or computer network
- Using a computer to access information using deception
- Theft of computer services
- Personal trespass by computer
- Using a computer to harass another

Computer Trespass

18.2-152.4 - Prohibits Computer Trespass

Class 1 misdemeanor for any person with malicious intent, to do any of the following:

Class 6 Felony if any actions cause damage valued at $1000

- Temporarily or permanently remove, halt, or disable any computer data, computer programs or computer software from a computer or computer network;
- Cause a computer to malfunction, regardless of how long the malfunction persists;
- Alter, disable, or erase any computer data, computer programs, or computer software;
- Effect the creation or alteration of a financial instrument or of am electronic transfer of funds
- Use a computer or computer network to cause physical injury to the property of another;
- Use a computer or computer network to make or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs, or computer software residing in, communicated by, or produced by a computer or computer network.

SPAM

- **18.2-152.3:1**- Prohibits SPAM, unsolicited bulk email or junk mail
- **Class 1 misdemeanor** to use a computer network with the *intent to falsify* or *forge* email transmission information in connection with the transmission of unsolicited bulk email (SPAM) through or into the computer network of an email service provider or its subscribers, or to *knowingly sell, give, or distribute or possess with the intent to sell, give, or distribute any software designed for this purpose*.

Harassment

18.2-152.7:1 – Harassment By Computer

- If any person with intent to coerce, intimidate, or harass any person
- Use a computer or computer network to *communicate obscene*, *vulgar*, *profane*, *lewd*, *lascivious*, or *indecent language*,
- Make any suggestions of *proposal* of an *obscene nature*, or *threaten* any illegal or immoral act,
- He shall be guilty of Class 1 misdemeanor

Threats

18.2-60 – Threats of death or bodily injury to a person or member of his family; threats to commit serious bodily harm to persons on school property

- Any person
- Knowingly communicates in writing, including an electronically transmitted communication producing a visual or electronic message
- A threat to kill or do bodily injury to a person or any member of his family
- On schools grounds, includes: bus, school sponsored activity
- Orally to any employee of school
- (Class 1 misdemeanor or Class 5 felony))

Cyber bullying

- Sending mean, vulgar, or threatening messages or images
- Posting sensitive, private information about another person
- Pretending to be someone else in order to make that person look bad
- Intentionally excluding someone from an online group

Cyber bullying can occur through:

- Emails
- Instant messaging
- Text or digital imaging messages sent on cell phones
- Web pages
- Blogs
- Chat rooms or discussion groups
- Other information communication technologies

Recent studies on cyber bullying

- 18% of students in grades 6-8 said they **had been cyber bullied** at least once in the last couple of months. (1 in 5)
- 11% of students in grade 6-8 said they **had cyber bullied** another person at least once in the last couple of months (1 in 10)
- 19% of regular internet users between the ages of 10 and 17 reported being involved in online aggression. (1 in 5)
- 17% of 6-11 year olds and 36% of 12-17 year olds reported that someone said threatening or embarrassing things about them through email, instant messages, websites, chat rooms, or text messages.

Sexting

•The act of text messaging

•Someone in the hopes of having a sexual encounter with them later;

•Initially casual, transitioning into highly suggestive, and even sexually explicit;

•Including the transmission of sexually explicit pictures via cell phone.

•Can occur via computer or cell phone

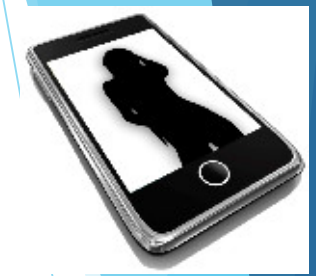
SEXTING

- Is a sexual revolution underway, with kids using photos as a sort of mating call, or as a kind of “modern day flirting?”

- Is sexting just today’s version of streaking, skinny-dipping, or mooning?

- Clearly, sexting can have tragic consequences, as shown in the case of Jessica Logan, who killed herself after her boyfriend circulated photos she’d sent to him.

SEXTING



Peer pressure influences girls who sext:

- Some 51% of teen girls say pressure from a male is a factor,

- Compared with 18% of boys who blame the opposite sex, according to the on-line survey last year of 1,280 people.

- Getting attention may be another motivation; two-thirds of teen girls and boys alike also said in the same survey that they use sexting to be “fun or flirtatious.”

What are the possible consequences of sexting?

- Embarrassment: when the "trusted" person you send the picture to sends it to others
- The picture ending up on the Internet for ALL to see
- Once the picture is sent it is out there FOREVER

What if a sexual predator get hold of the picture?

Would you like someone pleasuring himself to a picture of you?

Legal Ramifications

Can be criminally charged with Child Pornography or related violations

A sexually explicit picture of a person under the age of 18 = Child Pornography

- **The person taking the picture can be charged with Manufacturing Child Pornography**
- **Transmitting the picture is Distribution of Child Pornography**
- **The person receiving the picture can be charged with Possession of Child Pornography**
- **The person asking for the picture can be charged with Solicitation of the Manufacture of Child Pornography**

If convicted of child pornography or other related charges:

- All charges are Felonies
- Some carry sentences of up to 20 years
- Some have mandatory minimum sentences of 5 years that the judge cannot suspend or reduce
- If convicted, you will be required to register with the Virginia Sex Offender Registry yearly

The Court,

if requested by the Commonwealth Attorney,

may try a child 14 and older as an adult

Dangers Online and Strategies for Staying Safe Online

- Emails from unknown persons or businesses

  Danger: Attachments have been known to contain computer viruses and worms that can damage your computer

Strategies:

- Do not open these emails at all
- Never open any attachments

"Phishing" is another form of SPAM that involves sending an email falsely claiming to be legitimate organization such as a bank, an internet provider, or Ebay

Dangers Online and Strategies for Staying Safe Online cont:

Danger: The sender asks the recipient to provide his or her password, SSN, bank account # or credit cards account #'s to "verify" information or take some action that appears legitimate.

- If the recipient provides this information, it can be used to steal his or her identity.

Strategies:

- Do not provide personal information in response to an unsolicited email.
- Do not reveal personal information online unless you are sure the web site is legitimate and security measures are actively protecting users

Instant Messaging ("IM")

Allows people to have conversations in "real time" through their computers.

The "Buddy list" allows you to tell whether a friend is online and available to chat.

Danger: IM can be used to cyber bully or to harass someone or to engage in inappropriate or sexually explicit conversations.

Strategies:

- IM only people you know in real life
- Use privacy settings, limit to buddy list
- Make sure others can't search for you by email address and username
- Know the blocking features

Posting Videos and Photographs Online

Webcams, cell phones, and digital cameras allow you to post videos, photographs, and audio files online are great for staying in touch with family and friends

Danger:

- Digital files can easily be saved and distributed to other people, beyond the circle of trusted friends and family intended
- Saving, sending, and posting any images that are sexually provocative or inappropriate may not only be embarrassing, but may also lead to legal problems and other consequences.
- Employers are increasingly checking the web for images of or information about job applicants
- Images posted by teens may be seen years later with embarrassing and damaging consequences.

Posting Videos and Photographs Online Cont:

Strategies:

- Assume that anything posted online is there FOREVER
- Ask yourself: Would I be embarrassed if my family or friends saw these pictures?
- Be aware of cameras field of vision
- Do not post identity-revealing or sexually provocative photographs
- Don't post photographs of friends without permission from their parents

Once posted you lose all control!

Ways to stay safe!

- Never post or share your personal information online
- Never share your passwords (parents only)
- Never respond to emails or text messages from unfamiliar persons
- Never enter and area that charges for services without getting parents permission 1st
- Never meet anyone FACE 2 FACE whom you only know online
- Talk to your parents or trusted adult!

- Potential employers may find the picture during a pre-employment Internet search.
- You may not be accepted to the college of your choice
- Student loans may be denied
- Scholarships may be withdrawn or denied
- You lose your right to vote
- You lose your right to possess a firearm

Complete

- Read “Safeguarding your stuff, my stuff, our stuff” pages 9-11
- Answer “Your Online Image” questions. Use complete sentences or it will not be graded
- Read “Get the Facts” page 14 in your notes
- Take the Internet Safety Quiz