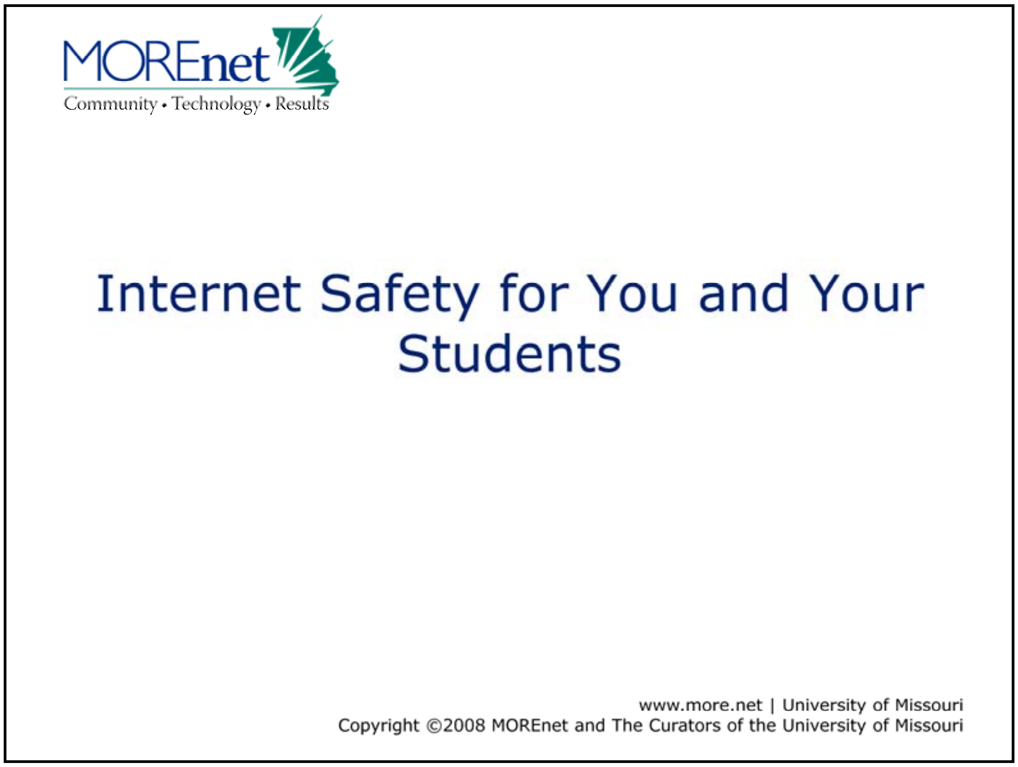
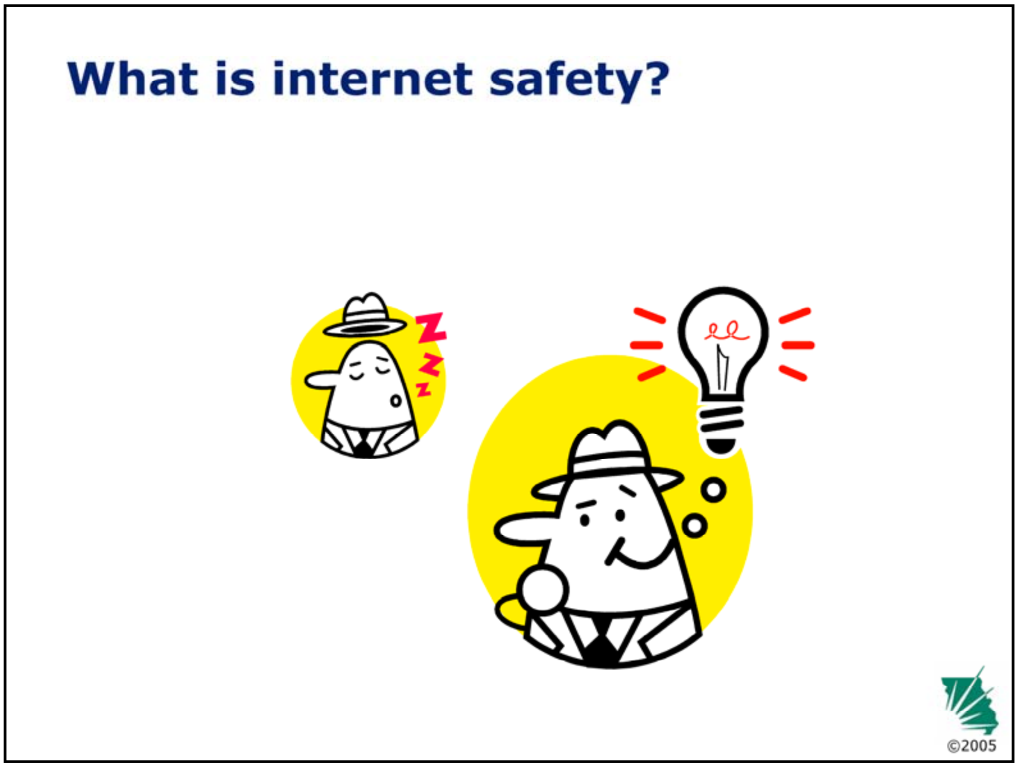


MOREnet
Community • Technology • Results

Internet Safety for You and Your Students

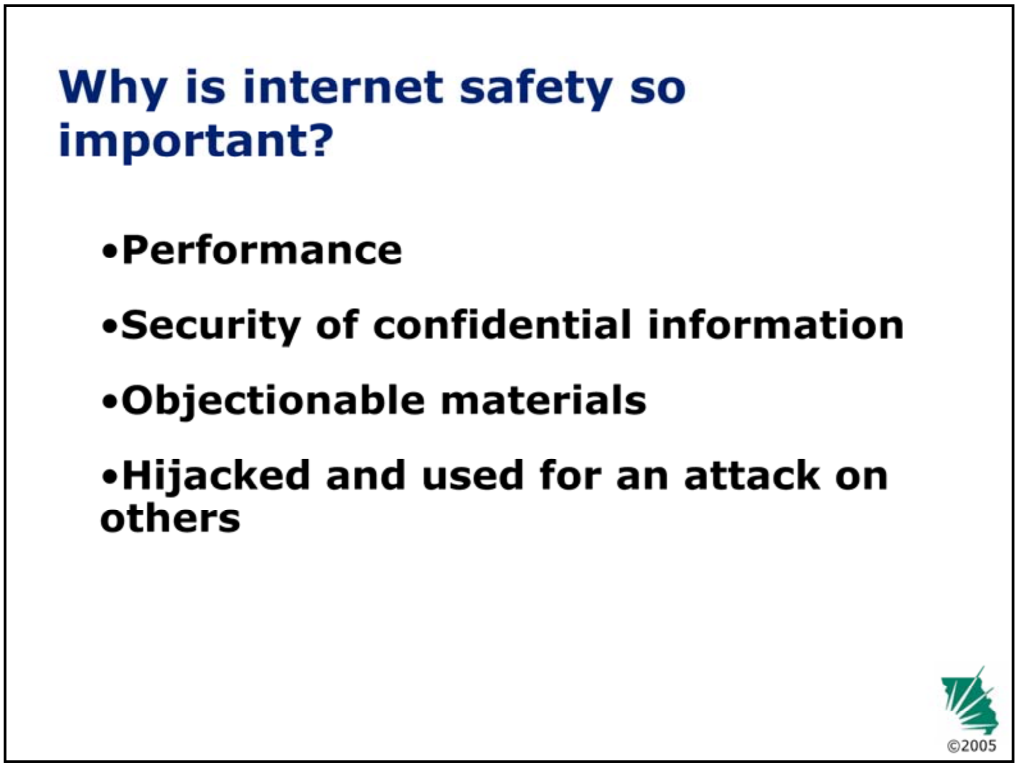
www.more.net | University of Missouri



What is internet safety?

©2005

What does internet safety mean to you?
Being safe on the internet means being security aware. Security awareness means understanding the various threats that exist in our environment and taking steps to guard against them.   Most people view security as a technical issue -- it's really a people issue. Security awareness helps people understand that there are things they can do to help.



Why is internet safety so important?

- Performance
- Security of confidential information
- Objectionable materials
- Hijacked and used for an attack on others

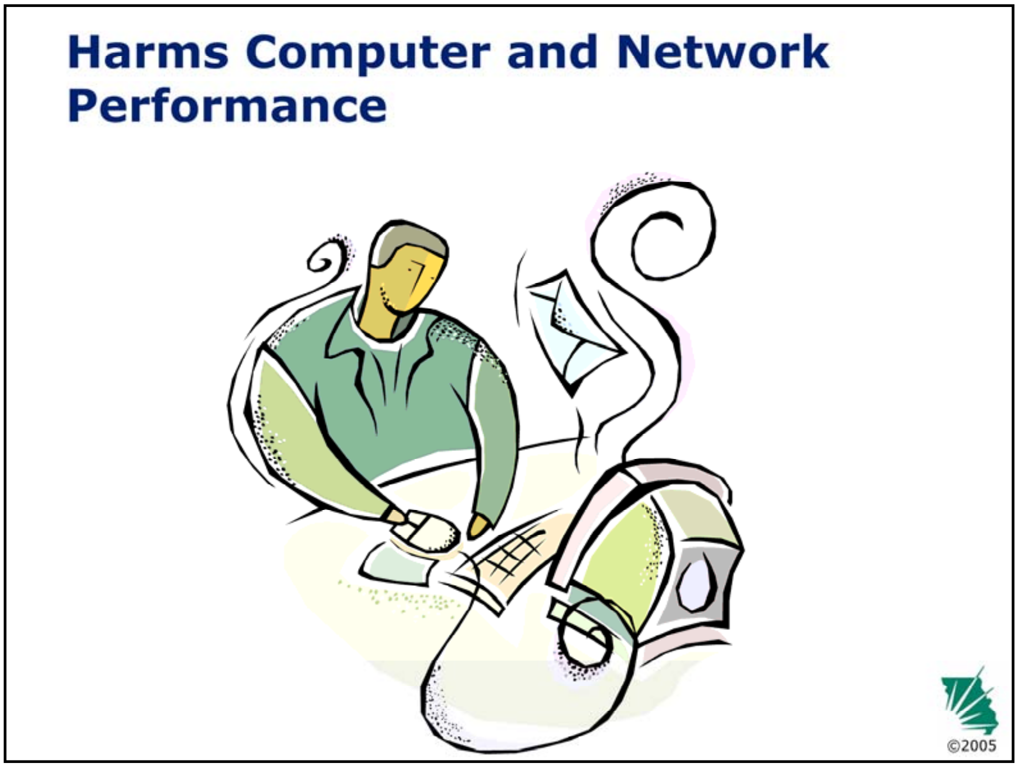
- Harms Computer and Network Performance
- Comprises the Security of confidential information
- Can be used to distribute objectionable materials
- computer can be hijacked and used to attack others

Help users avoid potential security risks.

Reduce the number of security incidents.

Less down time.

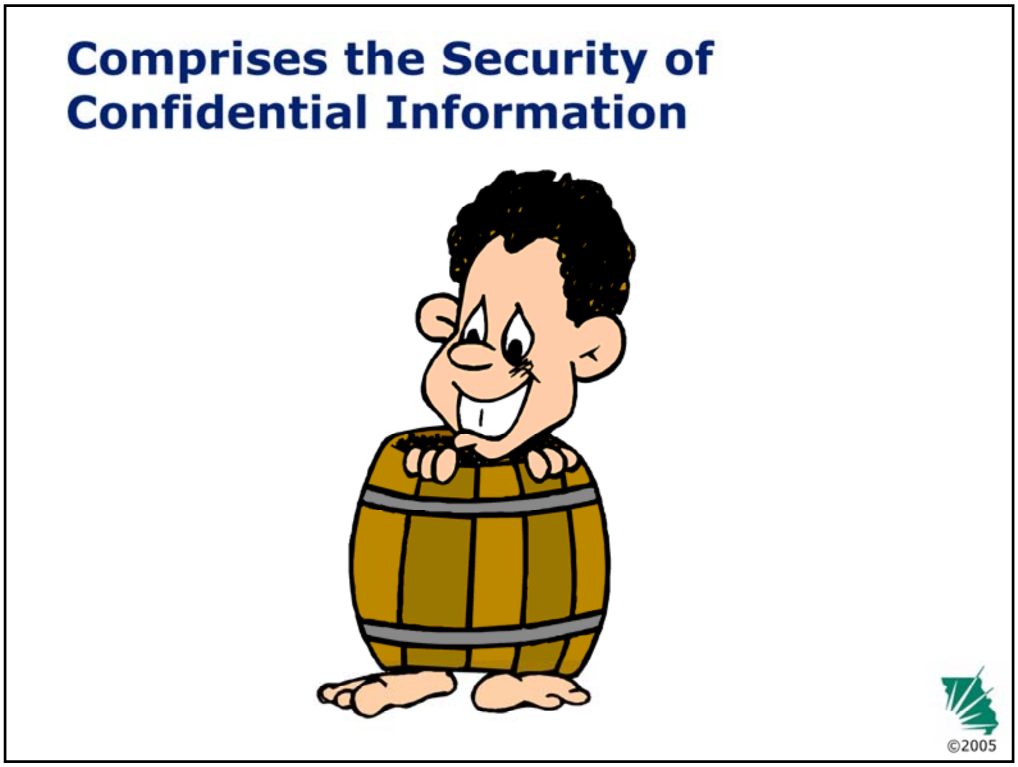
Better use of my network



Harms Computer and Network Performance

©2005

A computer, or a computer network, or both can have its performance and productivity seriously impaired by spyware, adware, malware, viruses, hijacking and hackers. These security issues increase the cost of your computer system due to unnecessary consumption of bandwidth, loss of productivity, and increased labor costs to troubleshoot.



Comprises the Security of Confidential Information

©2005

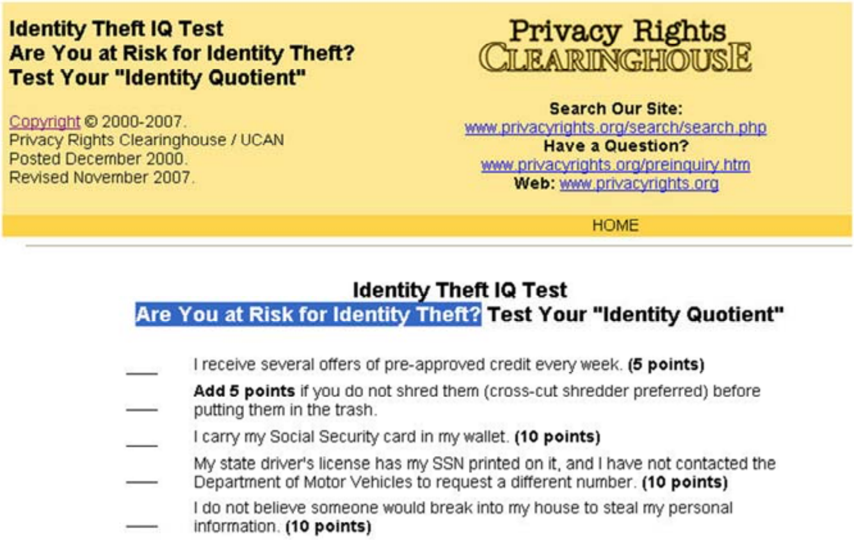
Hackers and spyware can compromise the security of confidential information. There are currently 26.7m Americans at risk from identity theft because they are unwittingly transmitting sensitive personal data to international hackers and criminals. http://www.scmagazine.com/us/news/article/523149/

The Anti-Phishing Working Group reported for the month of October 2005 that is had 15,820 phishing e-mail messages reported, 4367 unique phishing sites were identified, and 96 brand names were hi-jacked. The average time a site stayed on-line was 5.5 days. 43 percent of adults have received a phishing contact and of those, five percent gave their personal information.

www.informationweek.com/story/showArticle.jhtml?articleID=163101877&tid=13692

What is spyware? According to pcwebopedia it is any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can gather information about e-mail addresses, passwords and credit card numbers.

Are You at Risk for Identity Theft?



Identity Theft IQ Test
Are You at Risk for Identity Theft?
Test Your "Identity Quotient"

Copyright © 2000-2007.
Privacy Rights Clearinghouse / UCAN
Posted December 2000.
Revised November 2007.

Search Our Site:
www.privacyrights.org/search/search.php
Have a Question?
www.privacyrights.org/preinquiry.htm
Web: www.privacyrights.org

Identity Theft IQ Test
Are You at Risk for Identity Theft? Test Your "Identity Quotient"

___ I receive several offers of pre-approved credit every week. **(5 points)**

___ **Add 5 points** if you do not shred them (cross-cut shredder preferred) before putting them in the trash.

___ I carry my Social Security card in my wallet. **(10 points)**

___ My state driver's license has my SSN printed on it, and I have not contacted the Department of Motor Vehicles to request a different number. **(10 points)**

___ I do not believe someone would break into my house to steal my personal information. **(10 points)**

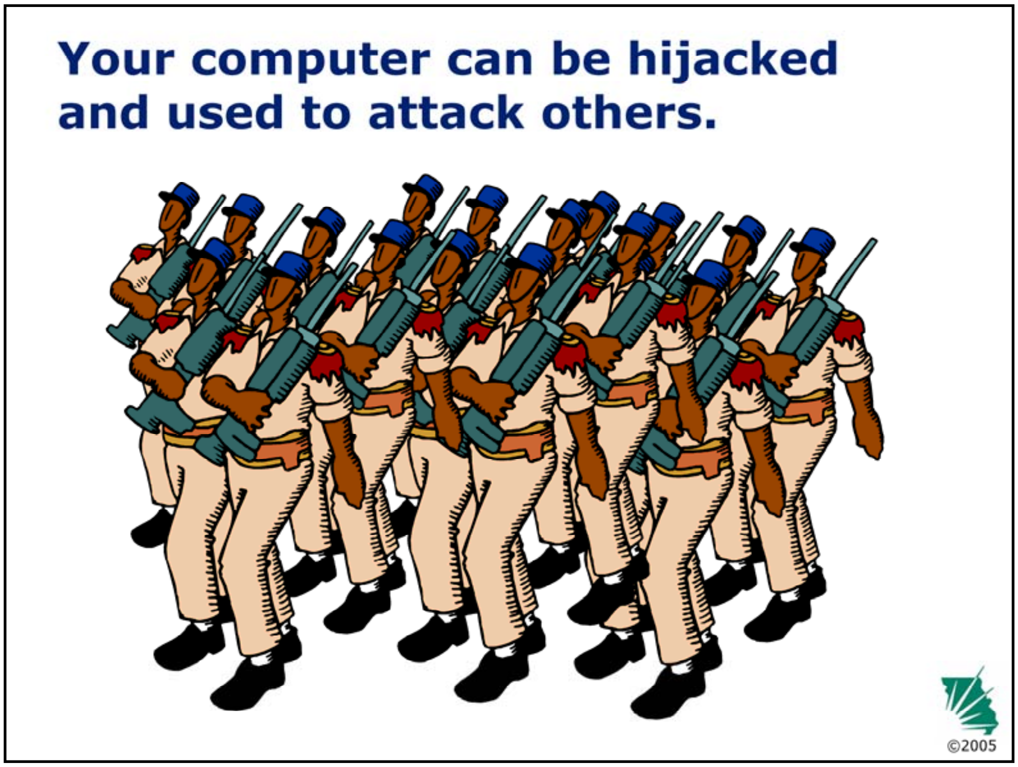
©2005

Go to the besafe.more.net on the right side click on identity theft IQ test and take the test

Can Be Used to Distribute Objectionable Materials

©2005

Many hackers hack to get resources such as bandwidth and harddrive space to store and distribute obscene, objectionable, and even illegal materials. Pornography, pirated movies and music are often found on computers with out the owners knowledge or consent only because they have been hacked.

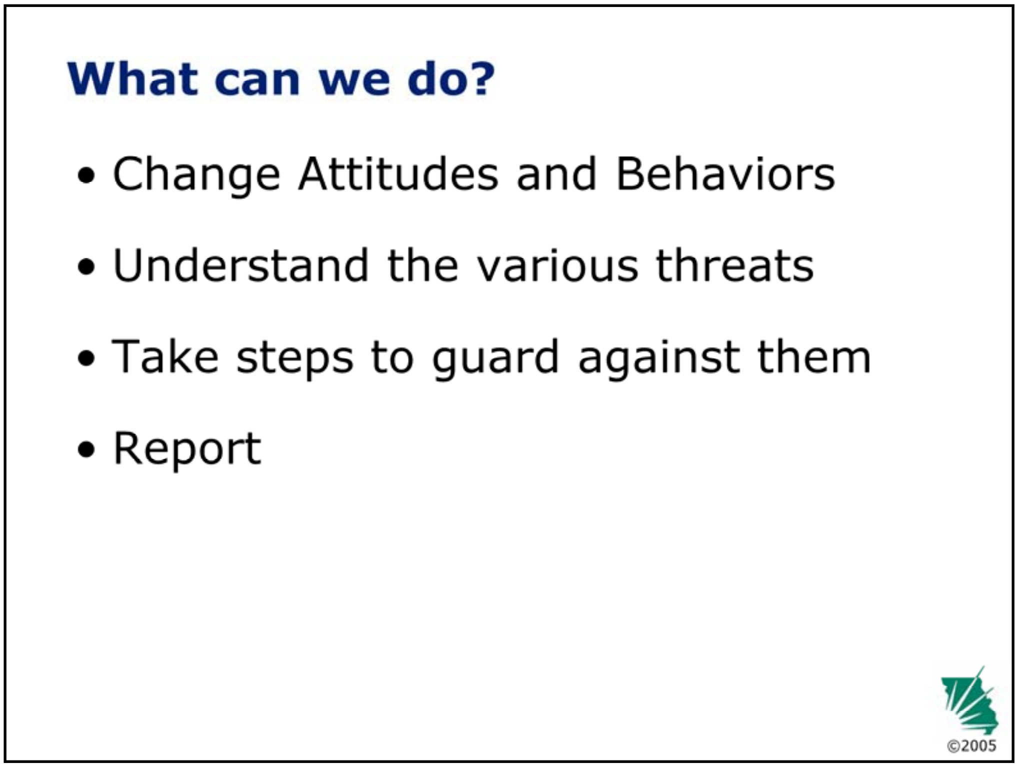


Your computer can be hijacked and used to attack others.

©2005

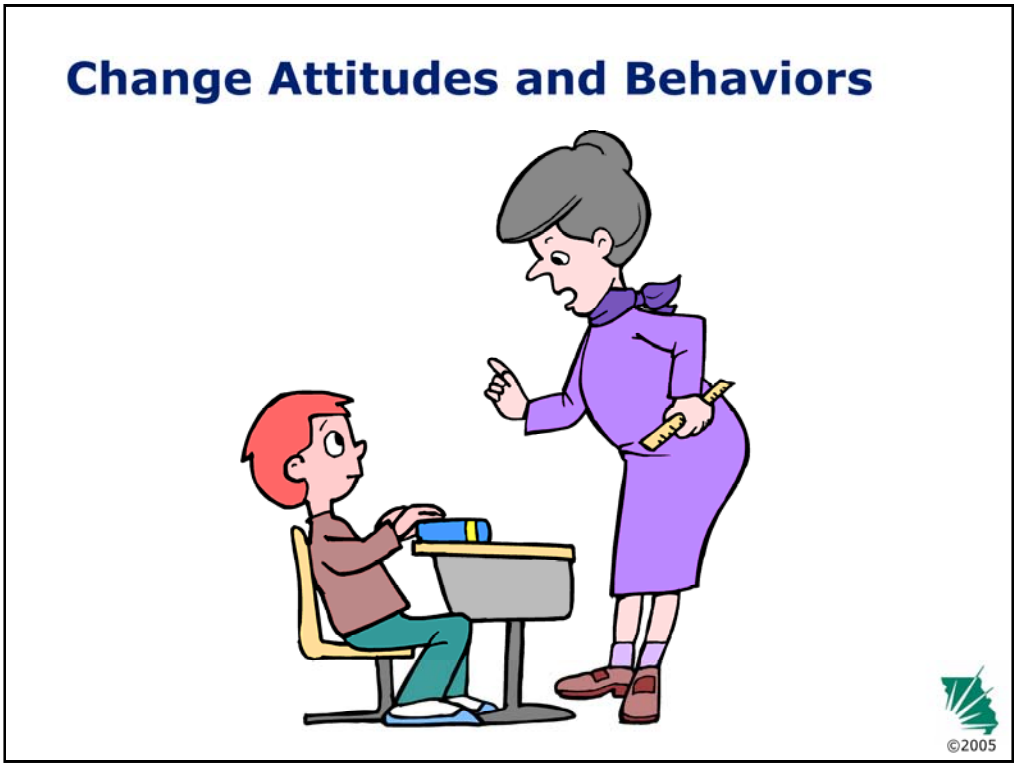
Allow a computer to be hijacked and used to attack a third party's computers in a distributed denial-of-service attack that can cost enterprises millions and expose them to legal liability

A Distributed Denial of Service, it is an attack where multiple compromised systems (which are usually infected with a Trojan) are used to target a single system causing it to crash. This “denial-of-service attack”, is a type of attack on a network that is designed to bring the network down by flooding it with useless traffic. Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack.



What can we do?

- Change Attitudes and Behaviors
- Understand the various threats
- Take steps to guard against them
- Report



Change Attitudes and Behaviors

©2005

Security is everyone’s responsibility.

As an employee of your organization, you have an obligation to act in its best interests. In addition, you should adhere to all policies and willingly comply with suggested best practices. Unfortunately, users often choose convenience over security.

Many of the problems stem from the following attitudes:

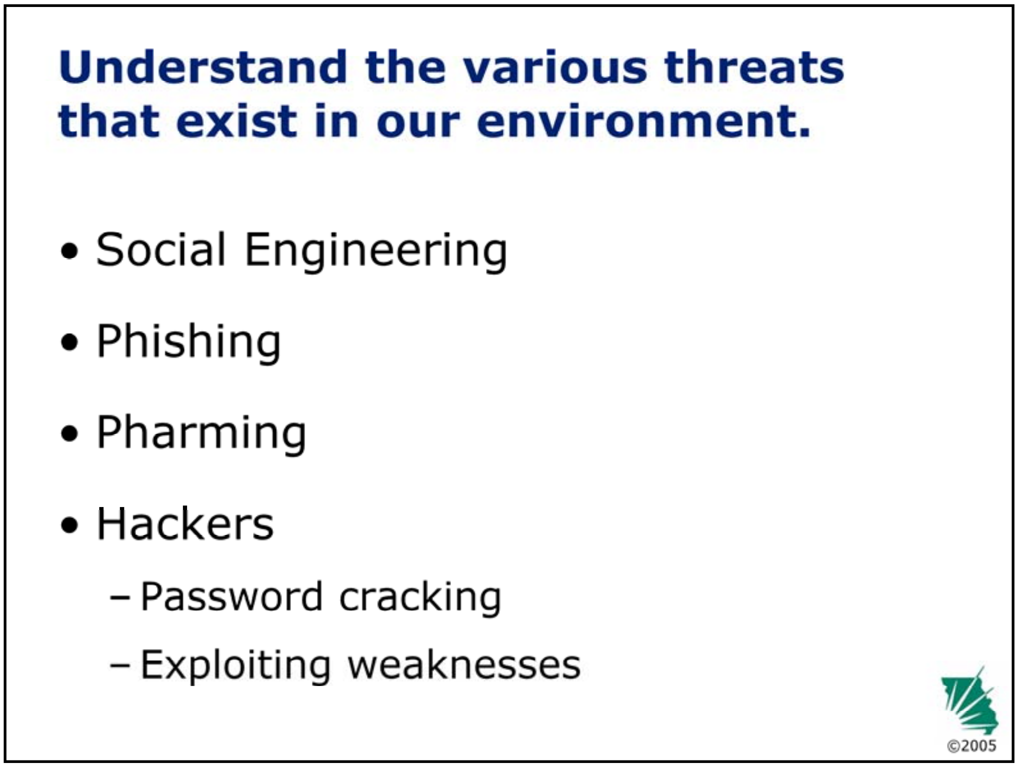
Security is the tech coordinator’s responsibility.

Security is an annoyance.

They don’t want me. I’m just a small fish.

It is to much trouble.

I’ve got “good” kids, patrons, coworkers. Etc.



Understand the various threats that exist in our environment.

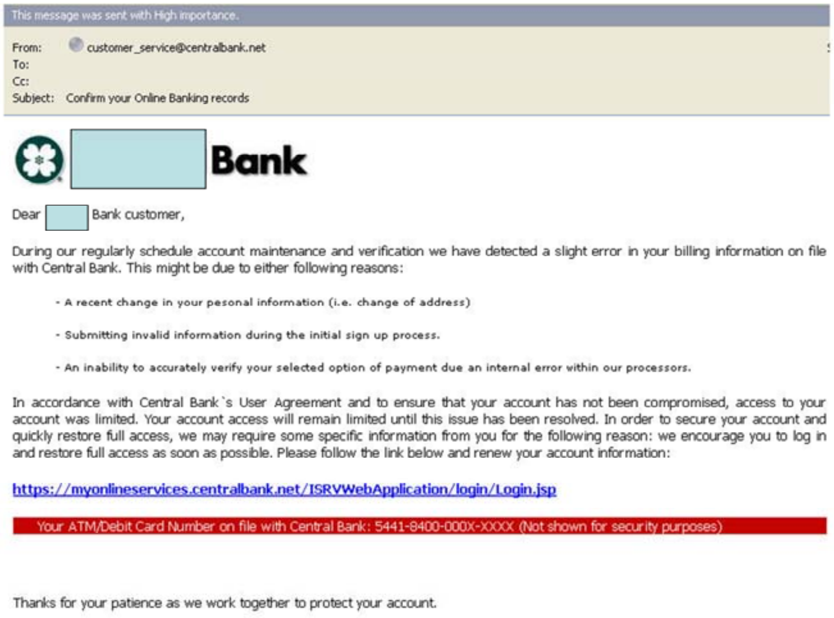
- Social Engineering
- Phishing
- Pharming
- Hackers
  - Password cracking
  - Exploiting weaknesses

Social Engineering

©2005

Social Engineering is the act of obtaining or attempting to obtain otherwise secure data by conning an individual into revealing secure information.
http://www.webopedia.com/TERM/s/social_engineering.html

Phishing



This message was sent with High importance.

From: customer_service@centralbank.net
To:
Cc:
Subject: Confirm your Online Banking records

[redacted] Bank

Dear [redacted] Bank customer,

During our regularly schedule account maintenance and verification we have detected a slight error in your billing information on file with Central Bank. This might be due to either following reasons:

- A recent change in your pesonal information (i.e. change of address)

- Submitting invalid information during the initial sign up process.

- An inability to accurately verify your selected option of payment due an internal error within our processors.

In accordance with Central Bank`s User Agreement and to ensure that your account has not been compromised, access to your account was limited. Your account access will remain limited until this issue has been resolved. In order to secure your account and quickly restore full access, we may require some specific information from you for the following reason: we encourage you to log in and restore full access as soon as possible. Please follow the link below and renew your account information:

https://myonlineservices.centralbank.net/ISRVWebApplication/login/Login.jsp

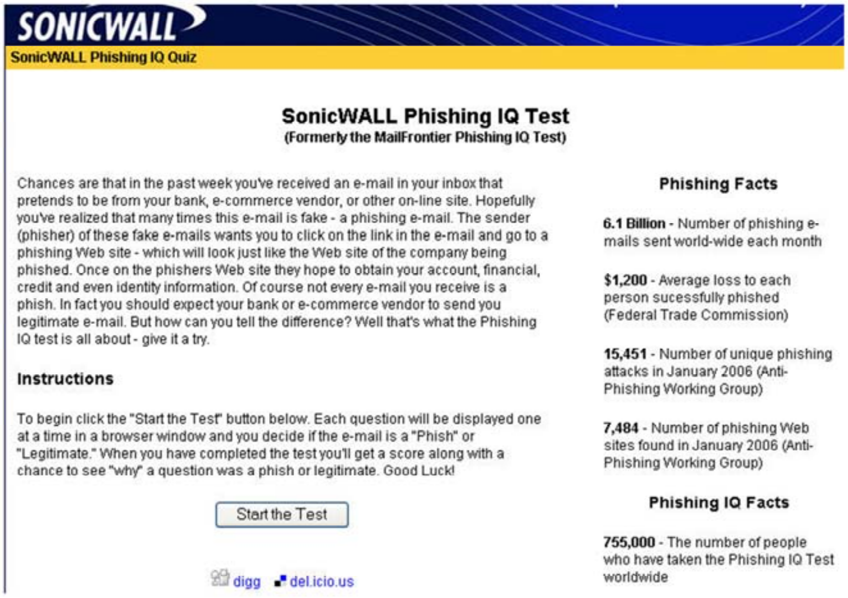
Your ATM/Debit Card Number on file with Central Bank: 5441-8400-000X-XXXX (Not shown for security purposes)

Thanks for your patience as we work together to protect your account.

Phishing it the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information. http://www.pcwebopedia.com/TERM/p/phishing.html. For the month of Oct 2005, 15,820 phishing e-mail messages were reported to the APWG, 4367 unique phishing sites were identified, and 96 brand names were hi-jacked.

Many phishing schemes are very obvious "The Nigeria Lottery", but many today are getting more and more sophisticated, using legitimate looking logos, and url's. They are also targeting certain times of the year to make them look more legitimate. (New Year, Fiscal year, new events such as a public computer error.)

Phishing Quiz



SONICWALL

SonicWALL Phishing IQ Quiz

SonicWALL Phishing IQ Test

(Formerly the MailFrontier Phishing IQ Test)

Chances are that in the past week you've received an e-mail in your inbox that pretends to be from your bank, e-commerce vendor, or other on-line site. Hopefully you've realized that many times this e-mail is fake - a phishing e-mail. The sender (phisher) of these fake e-mails wants you to click on the link in the e-mail and go to a phishing Web site - which will look just like the Web site of the company being phished. Once on the phishers Web site they hope to obtain your account, financial, credit and even identity information. Of course not every e-mail you receive is a phish. In fact you should expect your bank or e-commerce vendor to send you legitimate e-mail. But how can you tell the difference? Well that's what the Phishing IQ test is all about - give it a try.

Instructions

To begin click the "Start the Test" button below. Each question will be displayed one at a time in a browser window and you decide if the e-mail is a "Phish" or "Legitimate." When you have completed the test you'll get a score along with a chance to see "why" a question was a phish or legitimate. Good Luck!

Phishing Facts

6.1 Billion - Number of phishing e-mails sent world-wide each month

$1,200 - Average loss to each person sucessfully phished (Federal Trade Commission)

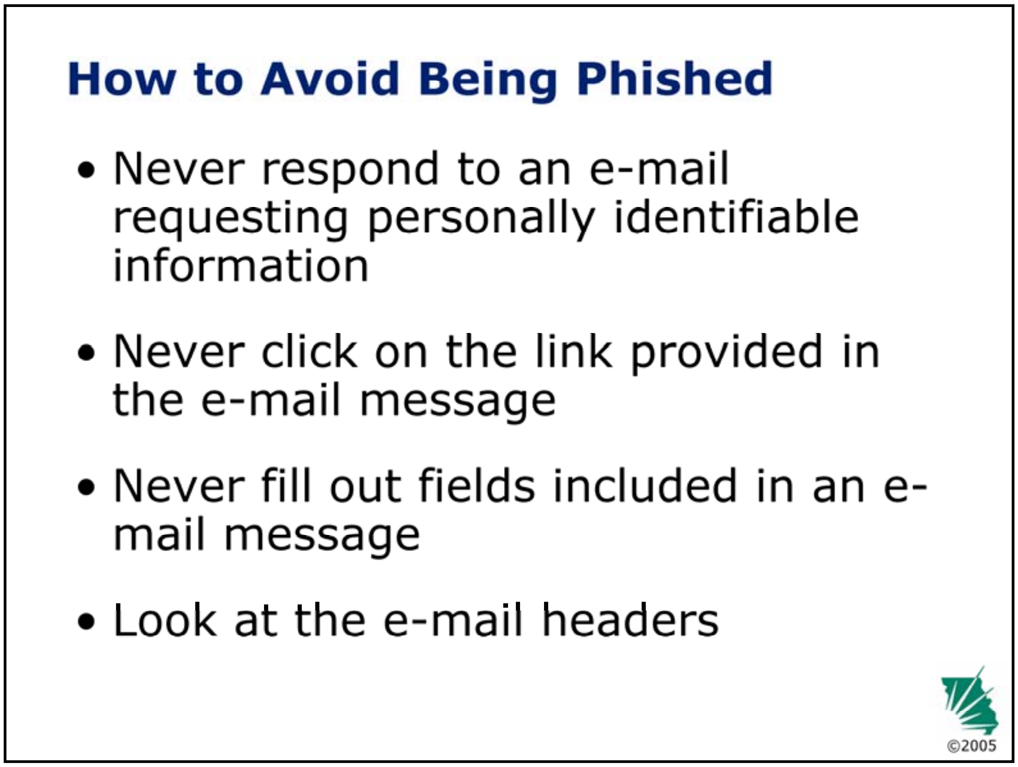
15,451 - Number of unique phishing attacks in January 2006 (Anti-Phishing Working Group)

7,484 - Number of phishing Web sites found in January 2006 (Anti-Phishing Working Group)

Phishing IQ Facts

755,000 - The number of people who have taken the Phishing IQ Test worldwide

http://www.sonicwall.com/phishing/



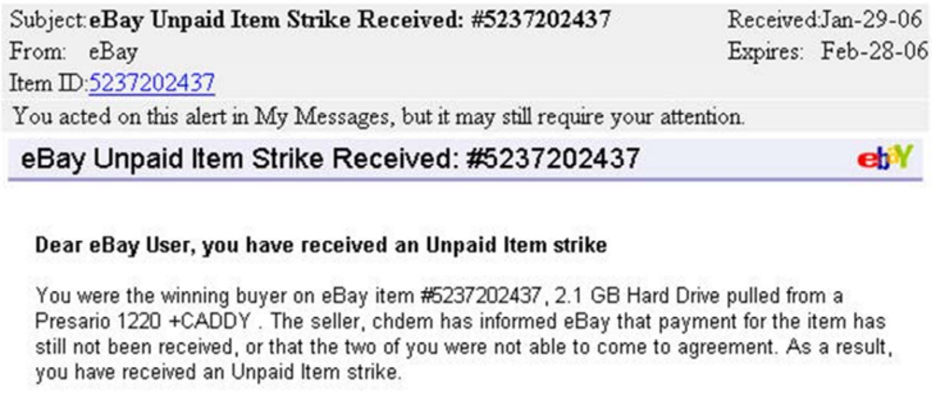
How to Avoid Being Phished

- Never respond to an e-mail requesting personally identifiable information
- Never click on the link provided in the e-mail message
- Never fill out fields included in an e-mail message
- Look at the e-mail headers

©2005

Look for misspellings inside the email, poor grammar, similar domain names, and requests for personal information.

I smell a Phish



Subject: **eBay Unpaid Item Strike Received: #5237202437** Received: Jan-29-06

From: eBay Expires: Feb-28-06

Item ID: 5237202437

You acted on this alert in My Messages, but it may still require your attention.

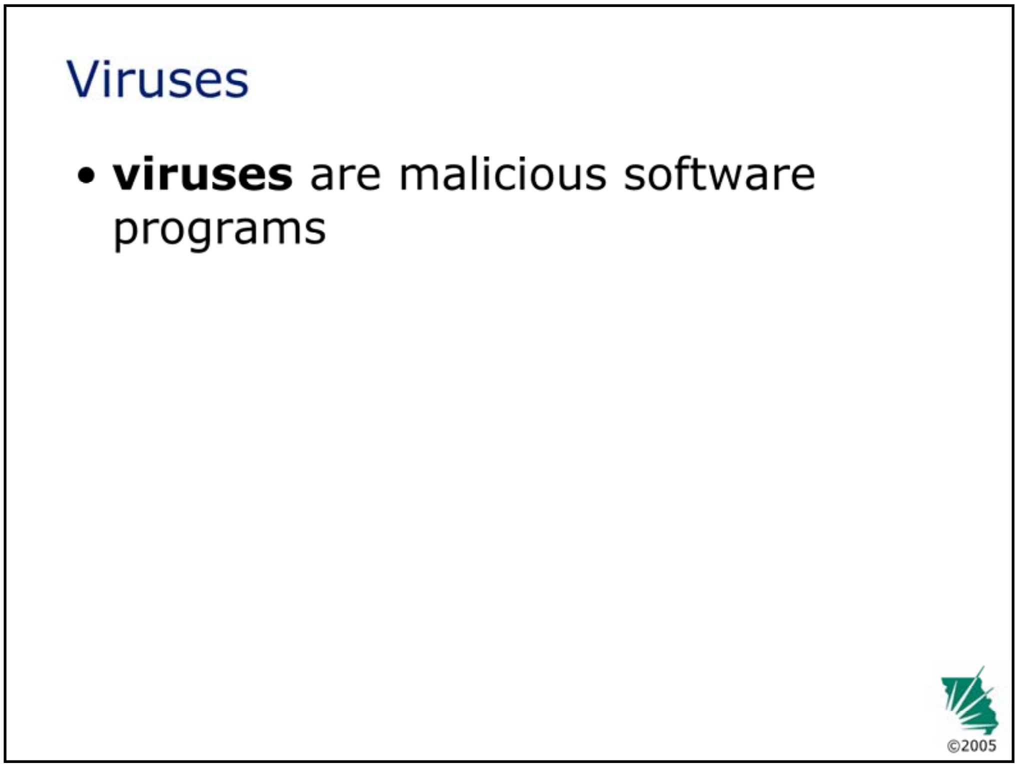
eBay Unpaid Item Strike Received: #5237202437

Dear eBay User, you have received an Unpaid Item strike

You were the winning buyer on eBay item #5237202437, 2.1 GB Hard Drive pulled from a Presario 1220 +CADDY . The seller, chdem has informed eBay that payment for the item has still not been received, or that the two of you were not able to come to agreement. As a result, you have received an Unpaid Item strike.

©2005

Many of these emails seemingly require immediate attention to protect your account, credit, et, and conveniently provide you a link to an area where the dispute can be resolved.



Viruses

- **viruses** are malicious software programs

©2005

viruses are malicious software programs, a form of **malware**. By definition, viruses exist on local disk drives and spread from one computer to another through sharing of "infected" files. Common methods for spreading viruses include floppy disks, FTP file transfers, and copying files between shared network drives. Once installed on a computer, a virus may modify or remove application and system files. Some viruses render a computer inoperable; others merely display startling screen messages to unsuspecting users. (1)

(1) http://compnetworking.about.com/cs/worldwideweb/g/bldef_virus.htm

How to avoid being infected

©2005

If you have a computer at home… YES, you need antivirus software. You can introduce infected files from your home machine to your work machine via floppy disk or flash drive.

Do not open mail from unknown senders

Be wary of clicking links in email and instant messages

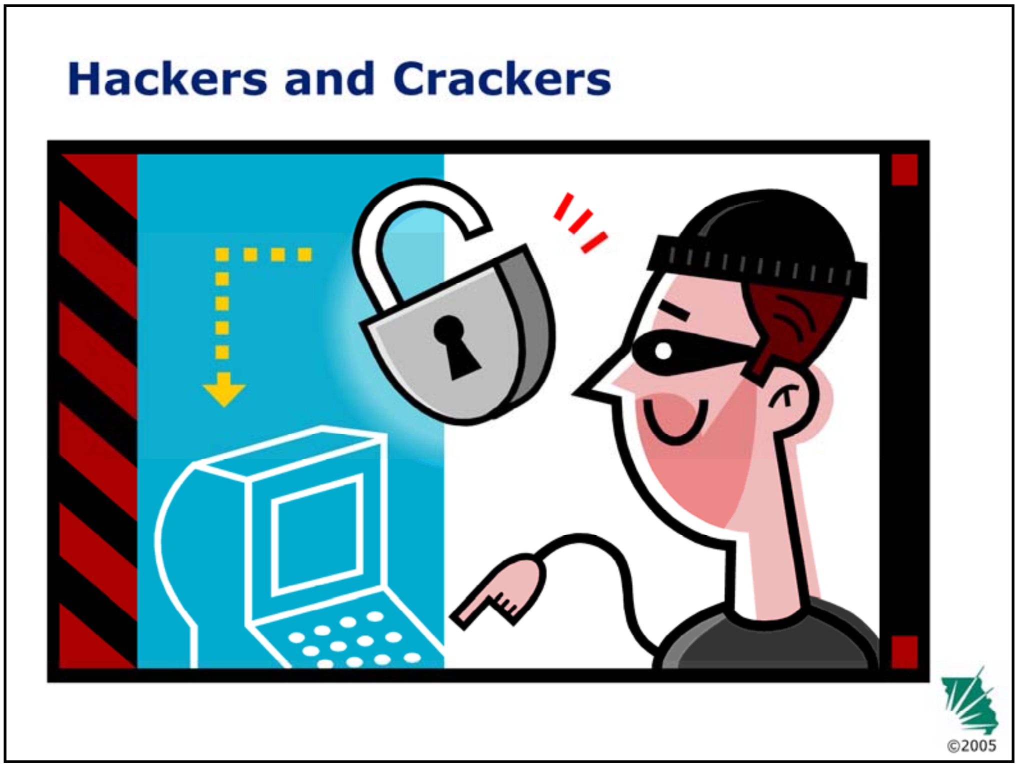
Keep your operating system and browser up to date

Only download software from websites you trust

Be cautious when clicking on pop-up advertisements

Be skeptical of offers that seem too good to be true

Whenever downloading or installing software, read the license agreement and policies carefully



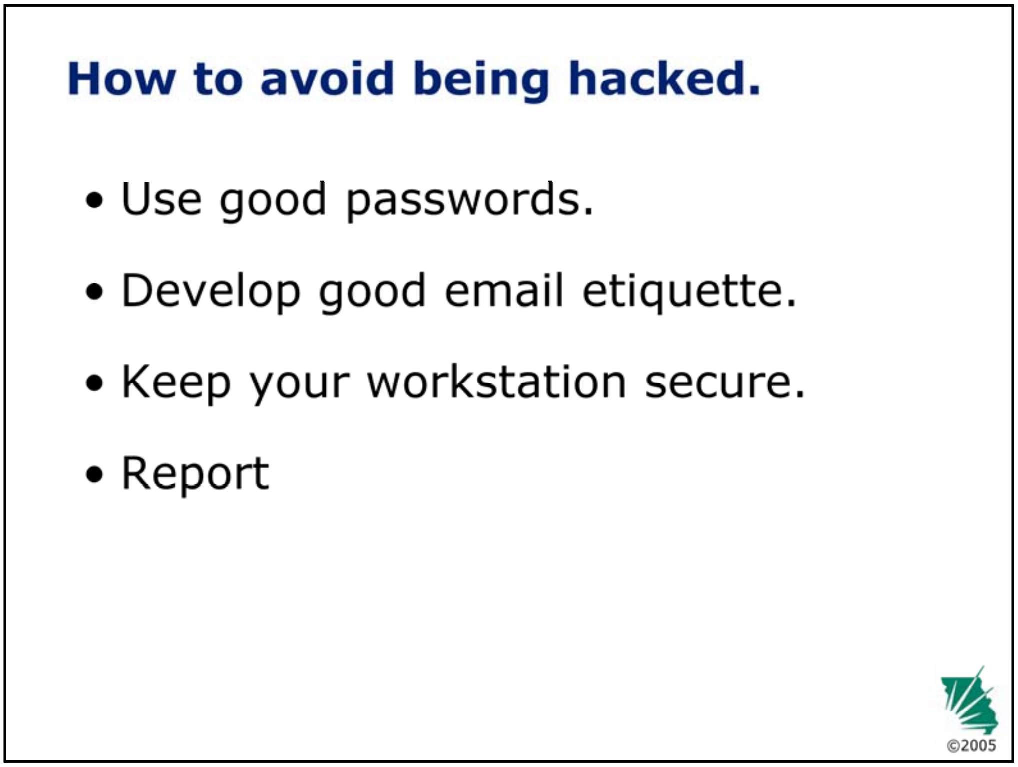
Hackers and Crackers

©2005

Hackers and Crackers have many ways to get into your system. Most involve exploiting vulnerabilities in the computers operating system and or weak or non existent passwords.

Hackers and Crackers have programs scanning the internet for unpatched computer operating systems. Once found the intruder can exploit the weakness for their own gain.

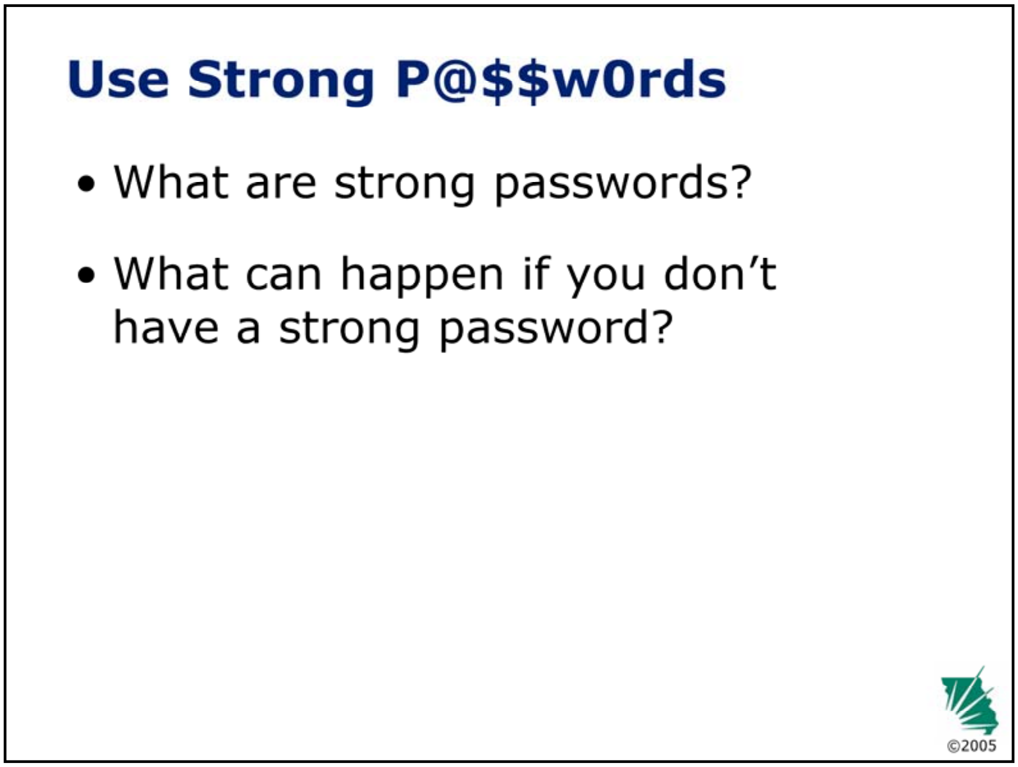
Password cracking is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system, typically, by repeatedly verifying guesses for the password. Three ways to get your password is by guessing, dictionary attacks, and brut force attacks.



How to avoid being hacked.

- Use good passwords.
- Develop good email etiquette.
- Keep your workstation secure.
- Report

©2005



Use Strong P@$$w0rds

- What are strong passwords?
- What can happen if you don’t have a strong password?

Also be aware of how many passwords do your users have? Usability versus security… If users have more than one password, they will typically use variations on the same password to make it easier to remember…. This will also make is easier to CRACK.

Strong passwords: How to create and use them

Published: March 22, 2006

Your passwords are the keys you use to access personal information that you've stored on your computer and in your online accounts. If criminals or other malicious users steal this information, they can use your name to open new credit card accounts, apply for a mortgage, or pose as you in online transactions. In many cases you would not notice these attacks until it was too late. Fortunately, it is not hard to create strong passwords and keep them well protected.

What makes a strong password

To an attacker, a strong password should appear to be a random string of characters. The following criteria can help your passwords do so:

Make it lengthy. Each character that you add to your password increases the protection that it provides many times over. Your passwords should be 8 or more characters in length; 14 characters or longer is ideal. Many systems also support use of the space bar in passwords, so you can create a phrase made of many words (a "pass phrase"). A pass phrase is often easier to remember than a simple password, as well as longer and harder to guess. **Combine letters, numbers, and symbols.** The greater variety of characters that you have in your password, the harder it is to guess. Other important specifics include:

The fewer types of characters in your password, the longer it must be. A 15-character password composed only of random letters and numbers is about 33,000 times stronger than an 8-character password composed of characters from the entire keyboard. If you cannot create a password that contains symbols, you need to make it considerably longer to get the same degree of protection. An ideal password combines both length and different types of symbols.

Use the entire keyboard, not just the most common characters. Symbols typed by holding down the "Shift" key and typing a number are very common in passwords. Your password will be much stronger if you choose from all the symbols on the keyboard, including punctuation marks not on the upper row of the keyboard, and any symbols unique to your language.

Use words and phrases that are easy for you to remember, but difficult for others to guess. The easiest way to remember your passwords and pass phrases is to write them down. Contrary to popular belief, there is nothing wrong with writing passwords down, but they need to be adequately protected in order to remain secure and effective. In general, passwords written on a piece of paper are more difficult to compromise across the Internet than a password manager, Web site, or other software-based storage tool, such as password managers.

Create a strong, memorable password in 6 steps

Use these steps to develop a strong password:

1. Think of a sentence that you can remember. This will be the basis of your strong password or pass phrase. Use a memorable sentence, such as "My son Aiden is three years old.“

2. Check if the computer or online system supports the pass phrase directly. If you can use a pass phrase (with spaces between characters) on your computer or online system, do so.

3. If the computer or online system does not support pass phrases, convert it to a password. Take the first letter of each word of the sentence that you've created to create a new, nonsensical word. Using the example above, you'd get: "msaityo".

4. Add complexity by mixing uppercase and lowercase letters and numbers. It is valuable to use some letter swapping or misspellings as well. For instance, in the pass phrase above, consider misspelling Aiden's name, or substituting the word "three" for the number 3. There are many possible substitutions, and the longer the sentence, the more complex your password can be. Your pass phrase might become "My SoN Ayd3N is 3 yeeRs old." If the computer or online system will not support a pass phrase, use the same technique on the shorter password. This might yield a password like "MsAy3yo".

5. Finally, substitute some special characters. You can use symbols that look like letters, combine words (remove spaces) and other ways to make the password more complex. Using these tricks, we create a pass phrase of "MySoN 8N i$ 3 yeeR$ old" or a password (using the first letter of each word) "M$8ni3y0".

6. Test your new password with Password Checker. Password Checker is a non-recording feature on this Web site that helps determine your password's strength as you type.

Password strategies to avoid

Some common methods used to create passwords are easy to guess by criminals. To avoid weak, easy-to-guess passwords:

Avoid sequences or repeated characters. "12345678," "222222," "abcdefg," or adjacent letters on your keyboard do not help make secure passwords.•

Avoid using only look-alike substitutions of numbers or symbols. Criminals and other malicious users who know enough to try and crack your password will not be fooled by common look-alike replacements, such as to replace an 'i' with a '1' or an 'a' with '@' as in "M1cr0$0ft" or "P@ssw0rd". But these substitutions can be effective when combined with other measures, such as length, misspellings, or variations in case, to improve the strength of your password.•

Avoid your login name. Any part of your name, birthday, social security number, or similar information for your loved ones constitutes a bad password choice. This is one of the first things criminals will try.•

Avoid dictionary words in any language. Criminals use sophisticated tools that can rapidly guess passwords that are based on words in multiple dictionaries, including words spelled backwards, common misspellings, and substitutions. This includes all sorts of profanity and any word you would not say in front of your children.•

Use more than one password everywhere. If any one of the computers or online systems using this password is compromised, all of your other information protected by that password should be considered compromised as well. It is critical to use different passwords for different systems.•

Avoid using online storage. If malicious users find these passwords stored online or on a networked computer, they have access to all your information.

The "blank password" option

A blank password (no password at all) on your account is more secure than a weak password such as "1234". Criminals can easily guess a simplistic password, but on computers using Windows XP, an account without a password cannot be accessed remotely by means such as a network or the Internet. (This option is not available for Microsoft Windows 2000, Windows Me, or earlier versions) You can choose to use a blank password on your computer account if these criteria are met:• You only have one computer or you have several computers but you do not need to access information on one computer from another one• The computer is physically secure (you trust everyone who has physical access to the computer) The use of a blank password is not always a good idea. For example, a laptop computer that you take with you is probably not physically secure, so on those you should have a strong password.

How to access and change your passwords

Online accounts

Web sites have a variety of policies that govern how you can access your account and change your password. Look for a link (such as "my account") somewhere on the site's home page that goes to a special area of the site that allows password and account management. Computer passwords

The Help files for your computer operating system will usually provide information about how to create, modify, and access password-protected user accounts, as well as how to require password protection upon startup of your computer. You can also try to find this information online at the software manufacturer's Web site. For example, if you use Microsoft Windows XP, online help can show you how to manage passwords, change passwords, and more Keep your passwords secret

Treat your passwords and pass phrases with as much care as the information that they protect. Don't reveal them to others. Keep your passwords hidden from friends or family members (especially children) who could pass them on to other less trustworthy individuals. Passwords that you need to share with others, such as the password to your online banking account that you might share with your spouse, are the only exceptions. Protect any recorded passwords. Be careful where you store the passwords that you record or write down. Do not leave these records of your passwords anywhere that you would not leave the information that they protect. Never provide your password over e-mail or based on an e-mail request. Any e-mail that requests your password or requests that you to go to a Web site to verify your password is almost certainly a fraud. This includes requests from a trusted company or individual. E-mail can be intercepted in transit, and e-mail that requests information might not be from the sender it claims. Internet "phishing" scams use fraudulent e-mail messages to entice you into revealing your user names and passwords, steal your identity, and more. Learn more about phishing scams and how to deal with online fraud.• Change your passwords regularly. This can help keep criminals and other malicious users unaware. The strength of your password will help keep it good for a longer time. A password that is shorter than 8 characters should be considered only good for a week or so, while a password that is 14 characters or longer (and follows the other rules outlined above) can be good for several years.•

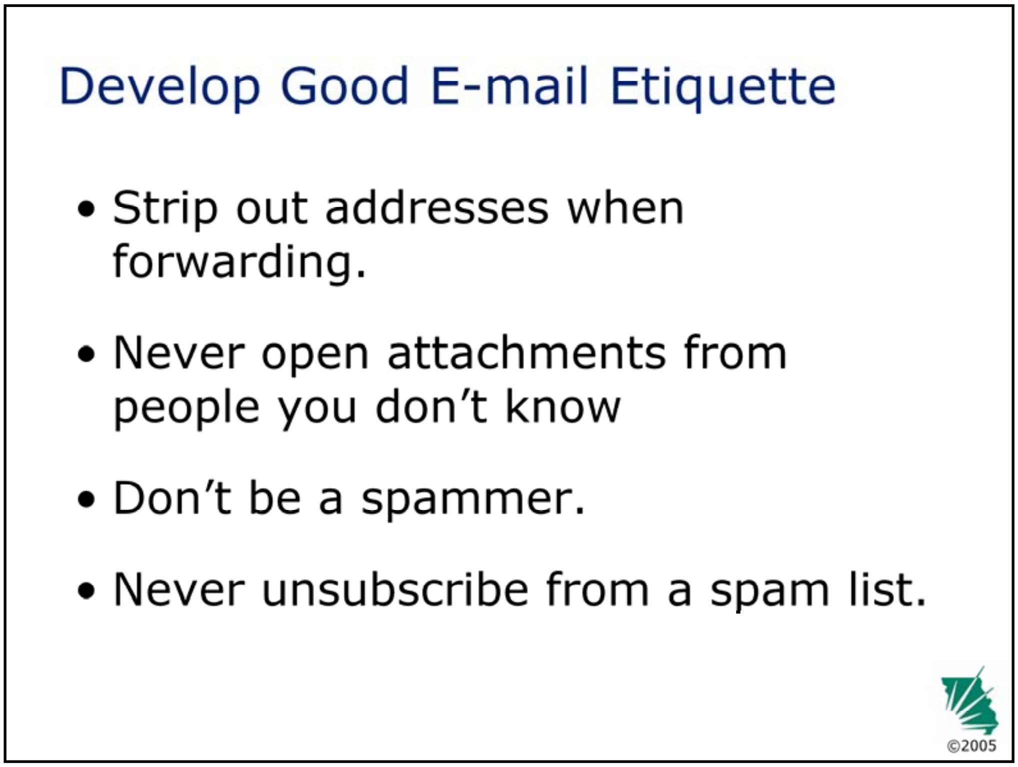
Do not type passwords on computers that you do not control. Computers such as those in Internet cafés, computer labs, shared systems, kiosk systems, conferences, and airport lounges should be considered unsafe for any personal use other than anonymous Internet browsing. Do not use these computers to check online e-mail, chat rooms, bank balances, business mail, or any other account that requires a user name and password. Criminals can purchase keystroke logging devices for very little money and they take only a few moments to install. These devices let malicious users harvest all the information typed on a computer from across the Internet—your passwords and pass phrases are worth as much as the information that they protect. What to do if your password is stolen

Be sure to monitor all the information you protect with your passwords, such as your monthly financial statements, credit, reports, online shopping accounts, and so on. Strong, memorable passwords can help protect you against fraud and identity theft, but there are no guarantees. No matter how strong your password is, if someone breaks into the system that stores it, they will have your password. If you notice any suspicious activity that could indicate that someone has accessed your information, notify authorities as quickly as you can. Get more information on what to do if you think your identity has been stolen or you've been similarly defrauded.

http://www.microsoft.com/protect/yourself/password/create.mspx

MICROSOFT AND/OR ITS RESPECTIVE SUPPLIERS MAKE NO REPRESENTATIONS ABOUT THE SUITABILITY OF THE INFORMATION CONTAINED IN THE DOCUMENTS AND RELATED GRAPHICS PUBLISHED AS PART OF THE SERVICES FOR ANY PURPOSE. ALL SUCH DOCUMENTS AND RELATED GRAPHICS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. MICROSOFT AND/OR ITS RESPECTIVE SUPPLIERS HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS WITH REGARD TO THIS INFORMATION, INCLUDING ALL WARRANTIES AND CONDITIONS OF MERCHANTABILITY, WHETHER EXPRESS, IMPLIED OR STATUTORY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL MICROSOFT AND/OR ITS RESPECTIVE SUPPLIERS BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF INFORMATION AVAILABLE FROM THE SERVICES.

THE DOCUMENTS AND RELATED GRAPHICS PUBLISHED ON THE SERVICES COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN. MICROSOFT AND/OR ITS RESPECTIVE SUPPLIERS MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED HEREIN AT ANY TIME.



Develop Good E-mail Etiquette

- Strip out addresses when forwarding.
- Never open attachments from people you don’t know
- Don’t be a spammer.
- Never unsubscribe from a spam list.

Don’t be a spammer….

©2005

Check out that email.

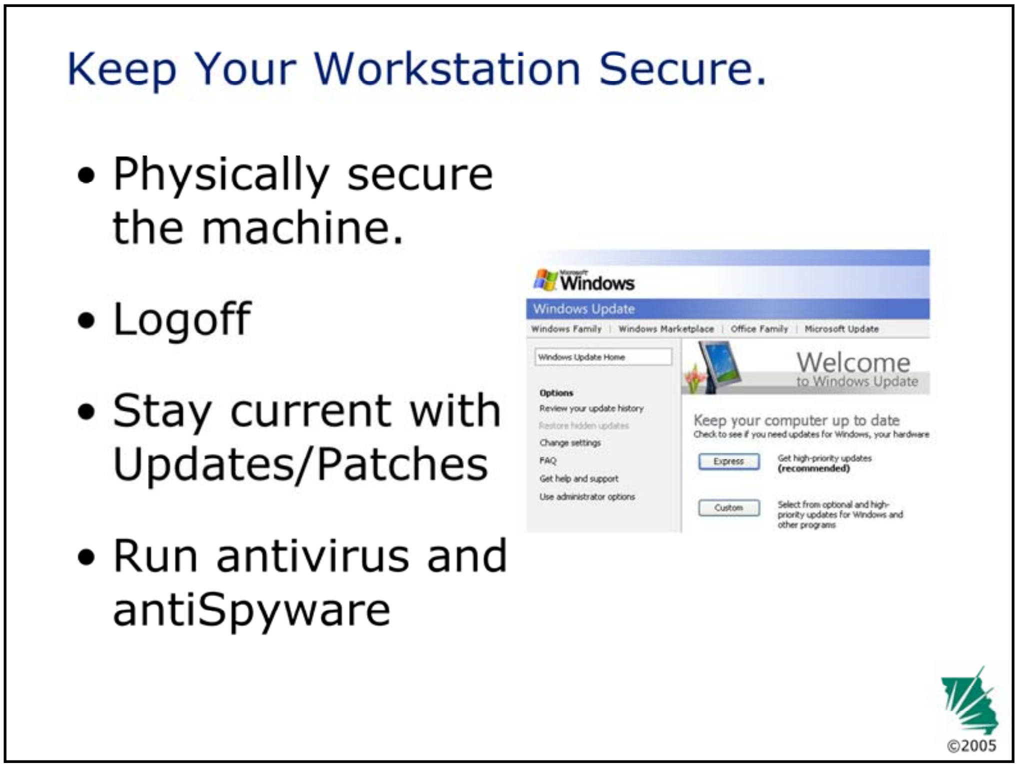
Hoax Resources

http:// www.snopes.com www.snopes.com

http://www.breakthechain.org/

http://hoaxbusters.ciac.org

http://www.synergypublishing.com/emailhoaxes.htm



Keep Your Workstation Secure.

- Physically secure the machine.
- Logoff
- Stay current with Updates/Patches
- Run antivirus and antiSpyware

Keep your computer up to date

Check to see if you need updates for Windows, your hardware

Get high-priority updates **(recommended)**

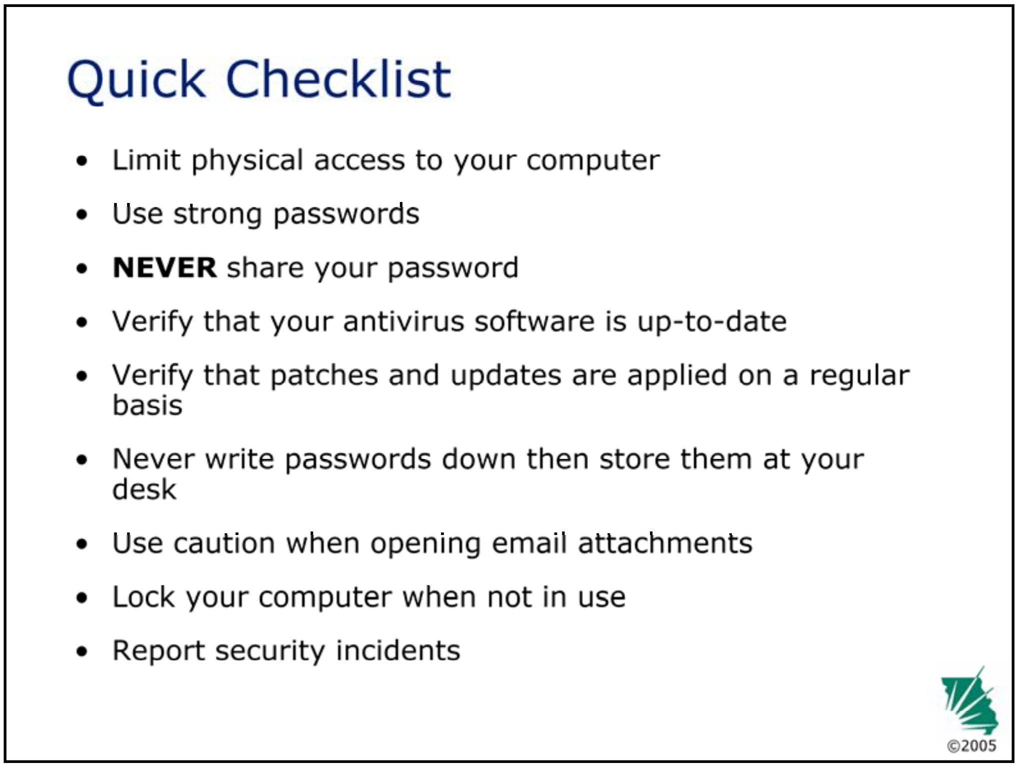
Select from optional and high-priority updates for Windows and other programs

Keep the computer in a secure location. Law #3 of Microsoft’s 10 Immutable Laws of Security says “If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.”

Be sure you logoff. No password is needed if you leave your workstation logged in.

Patch your systems. Most vulnerabilities in the computers operating system can be fixed by updating or patching the software. You should check for update or patches periodically to make sure you are not vulnerable. This includes other software on your computer especially antivirus and anti-spyware programs.

Run antivirus and antiSpyware. The number 1 law of Microsoft’s 10 Immutable Laws of Security says If a bad guy can persuade you to run his program on your computer, it’s not your computer anymore.



Quick Checklist

- Limit physical access to your computer
- Use strong passwords
- **NEVER** share your password
- Verify that your antivirus software is up-to-date
- Verify that patches and updates are applied on a regular basis
- Never write passwords down then store them at your desk
- Use caution when opening email attachments
- Lock your computer when not in use
- Report security incidents

What about your students?

©2005

Available Resources for Teaching Online Safety

©2005

According to surveys conducted by i-SAFE America, students across the country are engaging in risky behavior online.

39% have given out personal information (name, e-mail address, age, gender) online (when entering a contest, playing online games or signing up for websites).*

12% have met a new person from the Internet “face to face”.*

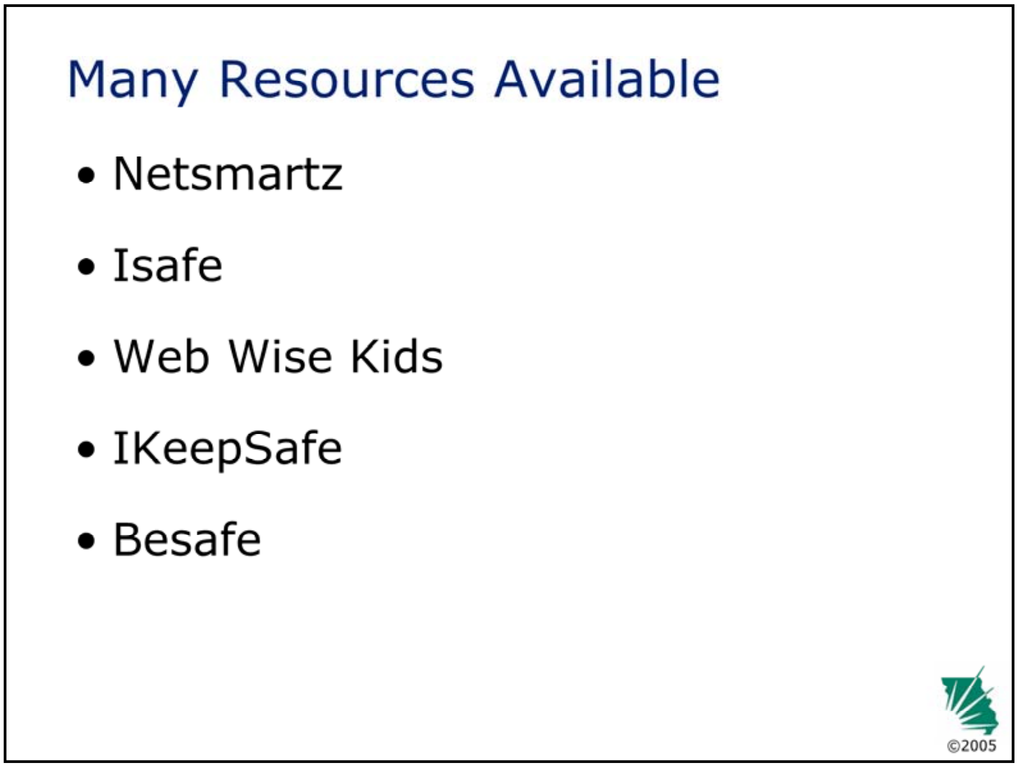
13% are willing to meet “face to face” with someone new they meet on the Internet.*

53% have seen something on the Internet that shouldn’t be on the Internet.**

64% know of or have heard about other students who have done something on the Internet that shouldn’t be done.*

* Combined 2003/2004 and 2004/2005 i-SAFE survey of 55,000 students

** 2004-05 i-SAFE survey of 36,000 students



Many Resources Available

- Netsmartz
- Isafe
- Web Wise Kids
- IKeepSafe
- Besafe

©2005

There are many excellent resources available to assist you in teaching internet safety. We will explore several.

Netsmartz

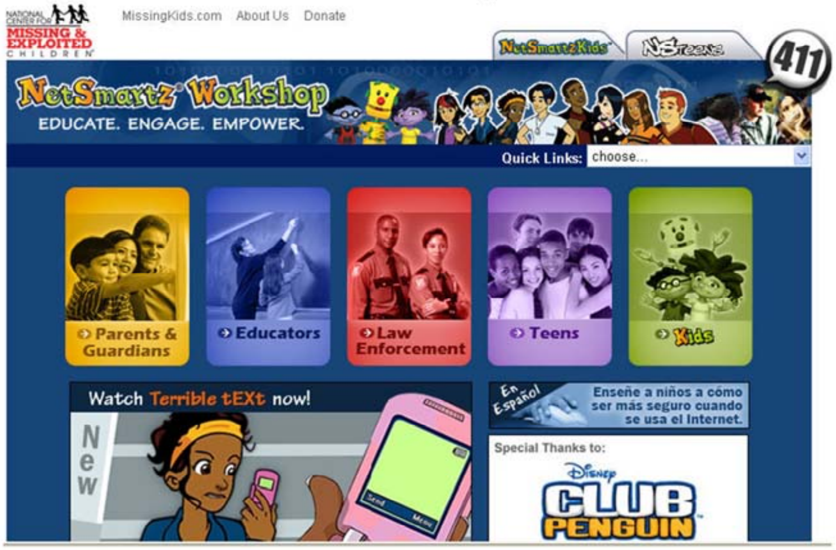
Isafe

Web Wise Kids

GetNetWise

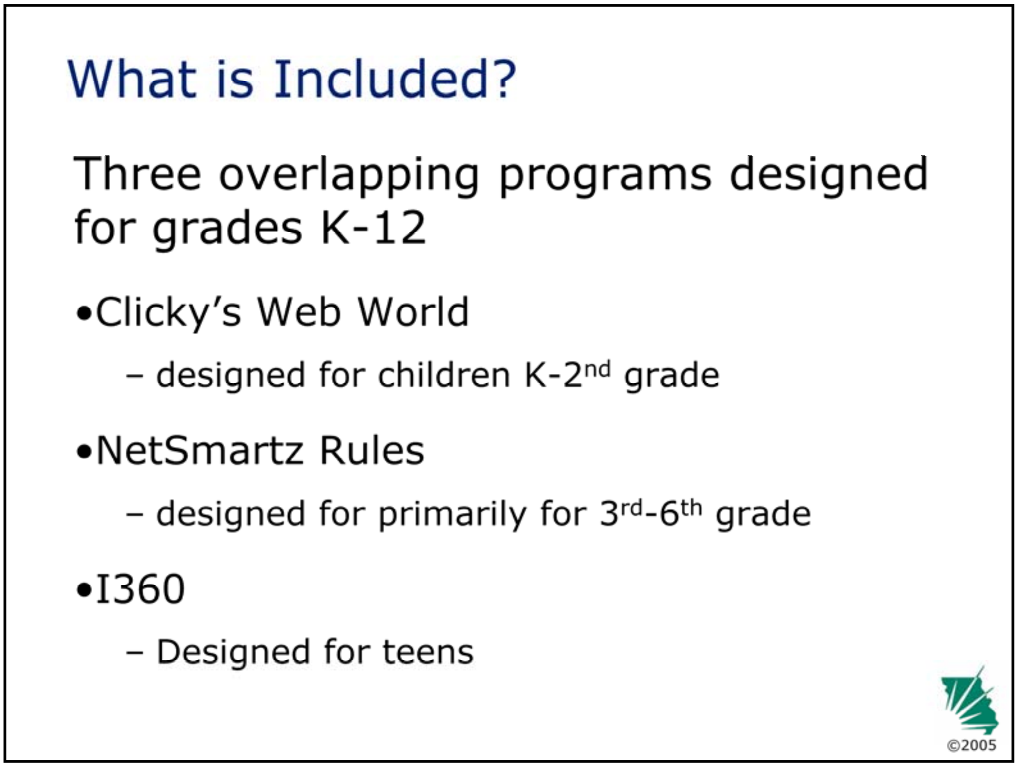
Play it Cybersafe

NetSmartz Workshop



©2005

The NetSmartz Workshop is an interactive, educational safety resource from the National Center for Missing & Exploited Children® (NCMEC) and Boys & Girls Clubs of America (BGCA) for children aged 5 to 17, parents, guardians, educators, and law enforcement that uses age-appropriate, 3-D activities to teach children how to stay safer on the Internet.



What is Included?

Three overlapping programs designed for grades K-12

- Clicky's Web World
  - designed for children K-2nd grade
- NetSmartz Rules
  - designed for primarily for 3rd-6th grade
- I360
  - Designed for teens

©2005

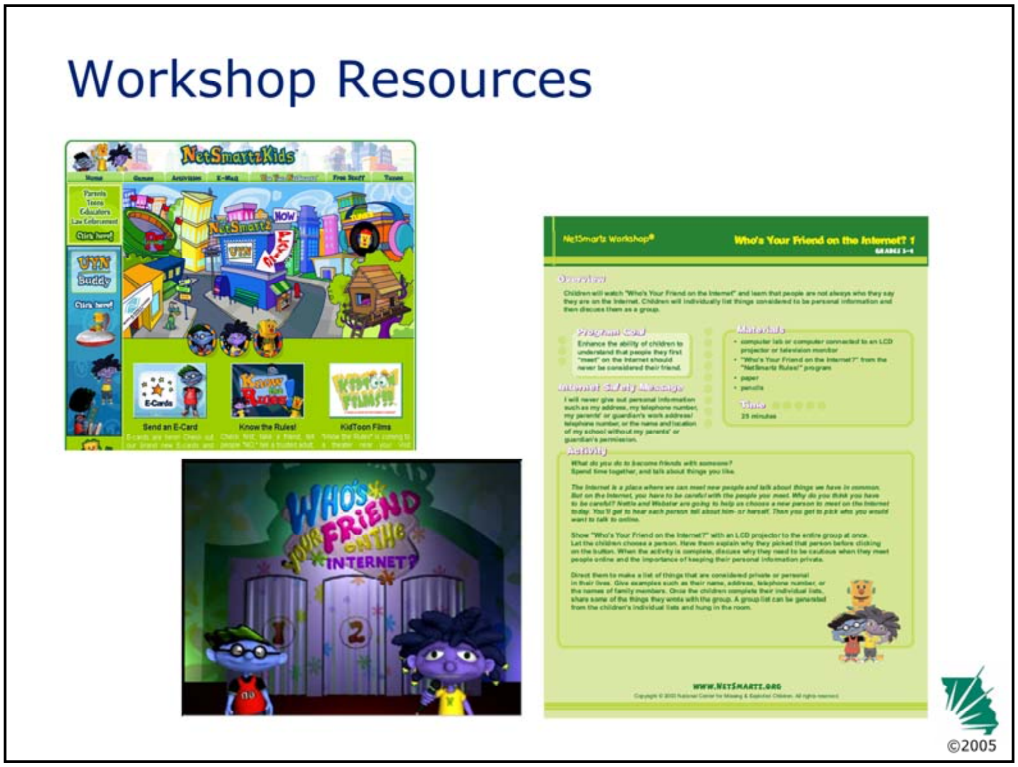
NetSmartz can be used online or downloaded onto a computer. The downloadable NetSmartz Workshop materials are a higher quality than what is available on the web and are run without Internet access. The downloadable version has the full-motion audio, video, and animation quality expected from a cartoon. These downloadable versions are available only to states that have an official partnership with NetSmartz.

Clicky's Web World is designed for children K-2nd grade and includes the character “Clicky”. He a web robot who helps to introduce us to the world of the Internet. He also teaches us how to avoid the Web Outlaws!

NetSmartz Rules! Is designed for primarily for 3rd-6th grade. Characters Nettie and her little brother Webster are “street-wise” about the Internet. They teach us about safety on the World Wide Web and how to watch out for the WYSIWYG's (what you see ISN'T what you get) of the Internet.

i-360 is an independent learning program including vignettes based on actual experiences to teach teens about Internet safety and the importance of good netiquette.

Workshop Resources



NetSmartz Workshop®

Who's Your Friend on the Internet? 1

GRADES 3–4

Overview

Children will watch "Who's Your Friend on the Internet" and learn that people are not always who they say they are on the Internet. Children will individually list things considered to be personal information and then discuss them as a group.

Program Goal

Enhance the ability of children to understand that people they first "meet" on the Internet should never be considered their friend.

Internet Safety Message

I will never give out personal information such as my address, my telephone number, my parents' or guardian's work address/telephone number, or the name and location of my school without my parents' or guardian's permission.

Materials

- computer lab or computer connected to an LCD projector or television monitor
- "Who's Your Friend on the Internet?" from the "NetSmartz Rules!" program
- paper
- pencils

Time

25 minutes

Activity

What do you do to become friends with someone?
Spend time together, and talk about things you like.

The Internet is a place where we can meet new people and talk about things we have in common. But on the Internet, you have to be careful with the people you meet. Why do you think you have to be careful? Nettie and Webster are going to help us choose a new person to meet on the Internet today. You'll get to hear each person tell about him- or herself. Then you get to pick who you would want to talk to online.

Show "Who's Your Friend on the Internet?" with an LCD projector to the entire group at once. Let the children choose a person. Have them explain why they picked that person before clicking on the button. When the activity is complete, discuss why they need to be cautious when they meet people online and the importance of keeping their personal information private.

Direct them to make a list of things that are considered private or personal in their lives. Give examples such as their name, address, telephone number, or the names of family members. Once the children complete their individual lists, share some of the things they wrote with the group. A group list can be generated from the children's individual lists and hung in the room.

WWW.NETSMARTZ.ORG

Activities – Interactive exercises that teach specific lessons about Internet safety.

Games – The games provided in the NetSmartz workshop are strictly for fun and incorporate the characters and concepts of Internet safety. There is no direct lesson taught through the games. They are to reinforce and make NetSmartz fun for kids.

Activity cards - Activity cards are designed to help you incorporate the NetSmartz online activities into your teachings. These cards were created by teachers for teachers to use. They will coordinate a classroom or lab activity with an online activity and provide ideas for discussion.

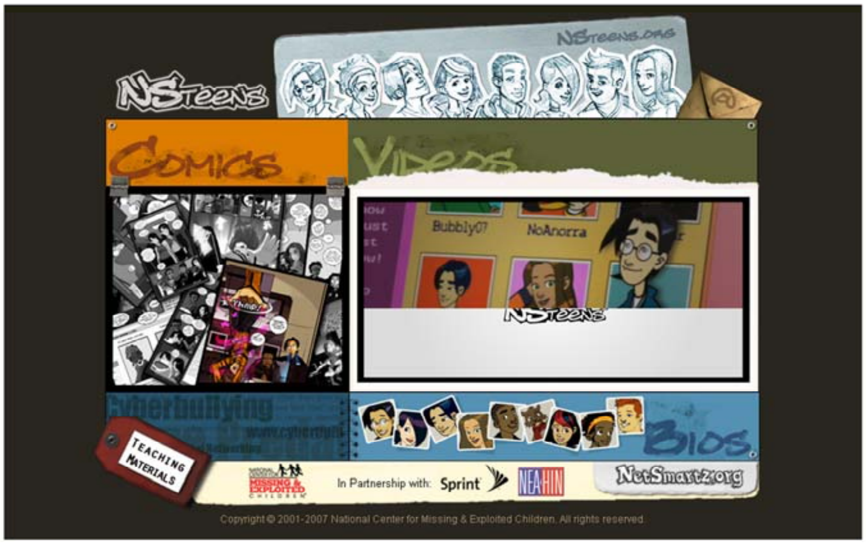
Internet safety certificates – These are downloadable certificates to be awarded upon completion of the corresponding program.

Web licenses – A license to be issued to those who complete the corresponding program, granting Internet privileges.

Internet safety pledges – Pledge to be signed by student and teacher/parent acknowledging Internet safety policy as set forth by NetSmartz.

Adventure games – Additional feature games where students can role play to stop Internet crimes and capture outlaws. There are two games designed for different age groups. Clicky's Quest and Derek in Distress.

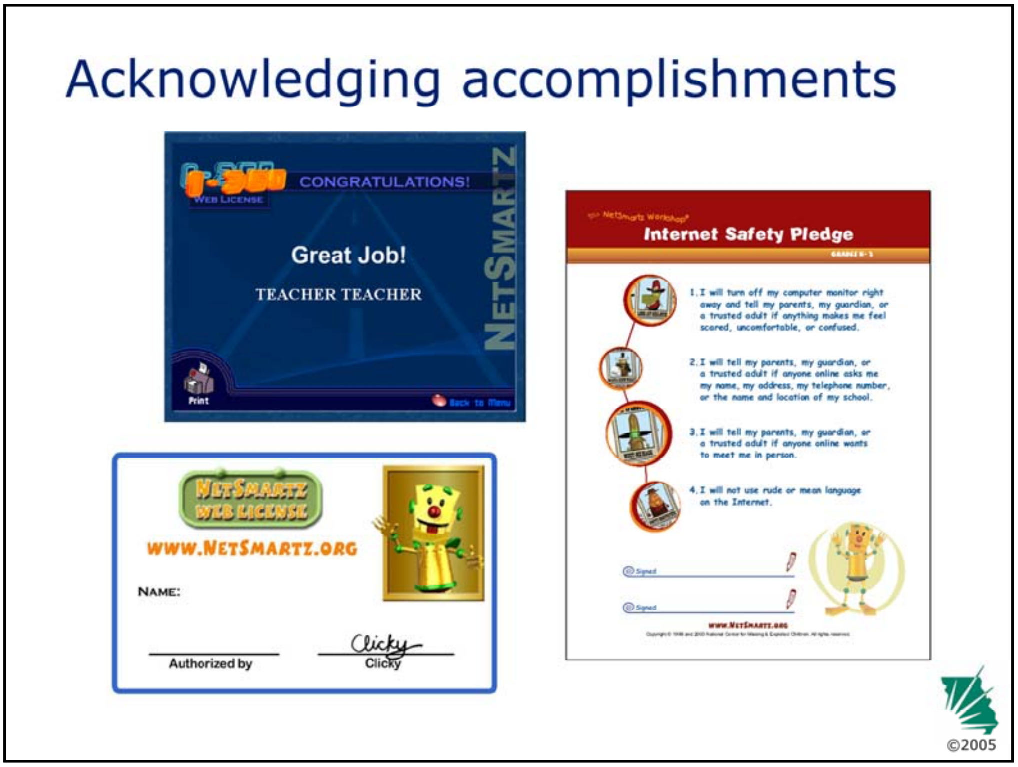
NS Teens



Copyright © 2001-2007 National Center for Missing & Exploited Children. All rights reserved.

©2005

Newer section for teens. In addition to other materials available, this section provides videos and a comic strip with information on topics like social networking and being safe with your information online.



Acknowledging accomplishments

i-SAFE WEB LICENSE CONGRATULATIONS!

Great Job!

TEACHER TEACHER

Print

Back to Menu

NETSMARTZ WEB LICENSE

WWW.NETSMARTZ.ORG

NAME:

Authorized by

Clicky

The NetSmartz Workshop®

Internet Safety Pledge

GRADES K-3

1. I will turn off my computer monitor right away and tell my parents, my guardian, or a trusted adult if anything makes me feel scared, uncomfortable, or confused.

2. I will tell my parents, my guardian, or a trusted adult if anyone online asks me my name, my address, my telephone number, or the name and location of my school.

3. I will tell my parents, my guardian, or a trusted adult if anyone online wants to meet me in person.

4. I will not use rude or mean language on the Internet.

Signed

Signed

WWW.NETSMARTZ.ORG

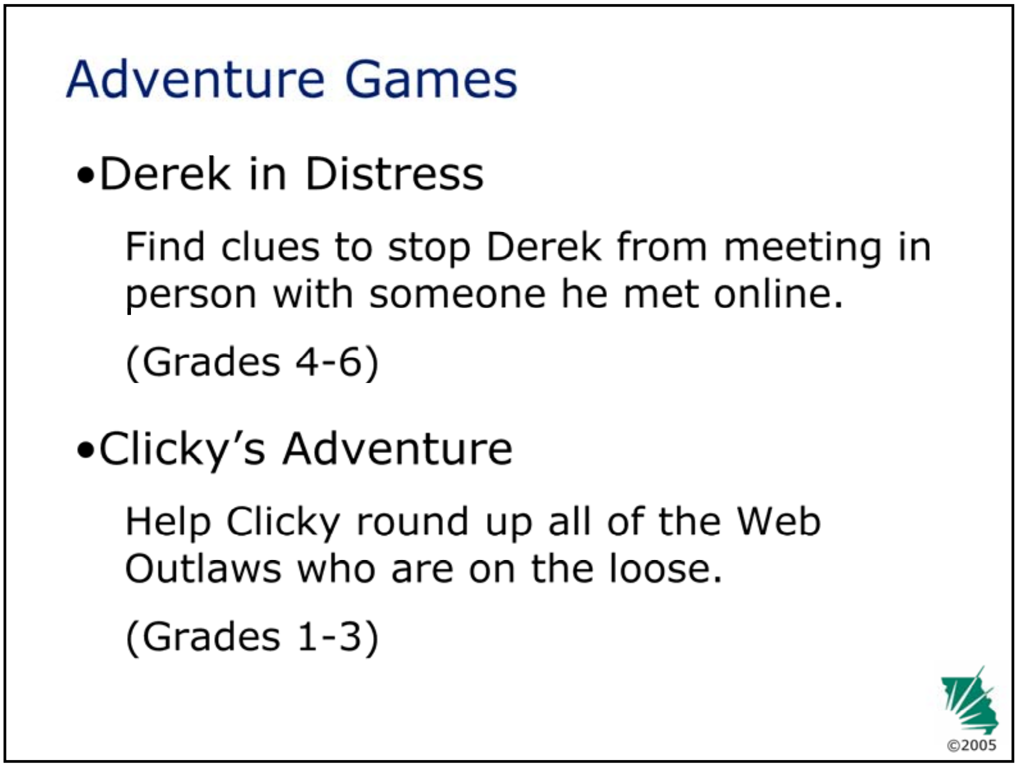
Copyright © 1998 and 2003 National Center for Missing & Exploited Children. All rights reserved.

©2005

Internet Safety Certificates - Internet Safety Certificates are downloadable certificates to be awarded upon completion of the corresponding program.

Web Licenses - A license to be issued to those who complete the corresponding program, granting Internet privileges.

Internet Safety Pledges - Pledge to be signed by student and teacher/parent acknowledging the Internet safety policy as set forth by NetSmartz.



Adventure Games

- Derek in Distress

  Find clues to stop Derek from meeting in person with someone he met online.

  (Grades 4-6)

- Clicky’s Adventure

  Help Clicky round up all of the Web Outlaws who are on the loose.

  (Grades 1-3)

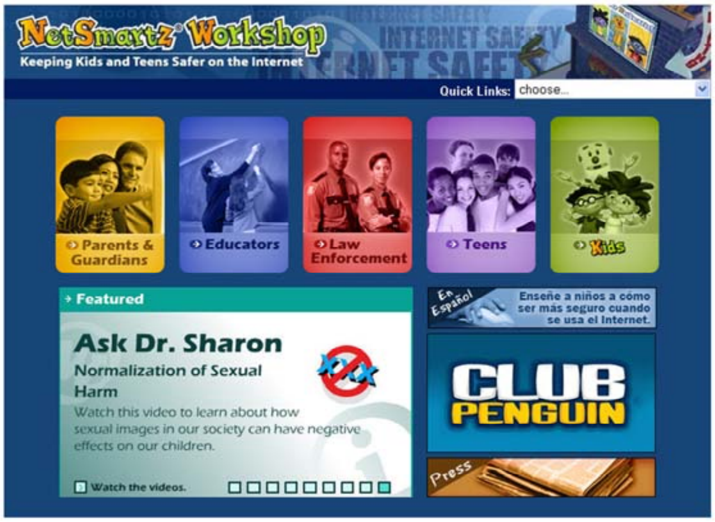
©2005

"NetSmartz Agents: Derek in Distress" Nicole is worried that her twin brother Derek may have left to meet in person with someone he first met online, so she has called in the NetSmartz Agents to help track him down. Children grades 4 through 6 can test their detective skills while learning about various Internet dangers as they search through the Washington D.C. area for clues and people that may lead them to find Derek before it's too late.

"Clicky's Quest" The mysterious Baron E. Vyle has released the Webville Outlaws to wreak havoc on the Internet. Help Agent Clicky recapture the Outlaws before it’s too late. Children grades 1 through 3 will enjoy multiple levels of game play as they learn what Internet dangers each of the four Outlaws represent and how to appropriately respond to those dangers.

Where is NetSmartz Available?

http://www.netsmartz.org



Ask Dr. Sharon

Normalization of Sexual Harm

Watch this video to learn about how sexual images in our society can have negative effects on our children.

©2005

Parents & Guardians - Communication is an effective tool for parents and guardians when helping their children avoid the dangers that exist on the Internet. NetSmartz provides on- and offline learning activities for parents to facilitate discussions with their children and teens about Internet safety.

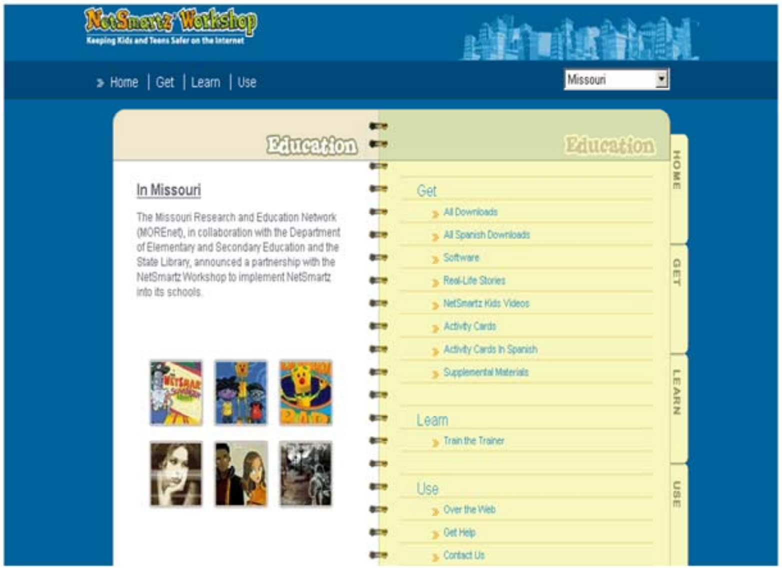
Educators - This page is designed to show educators and administrators how to use NetSmartz interactive materials in their classrooms, accumulate more information about Internet safety and technology, and take steps to bring their classrooms into the 21st century. Complete with downloadable programs for educators and links to national education standards..

Law Enforcement - NetSmartz offers a variety of resources to law enforcement to assist them in their efforts to keep their communities safer. Whether the presentation is 10 minutes long or 2 hours, for children or adults, NetSmartz resources can accommodate the circumstance.

Teens -Watch teens share their own "Real-Life Stories" about issues affecting them on the Internet such as cyberbullying, online enticement, and giving out too much personal information. Teen learn to use the CyberTipline to report any incidents of Internet exploitation.

Kids – Links users to the page containing activities and games for the Clicky's Web World and NetSmartz Rules programs. Kids can also e-mail the NetSmartz characters.

Where is NetSmartz Available?
State Intranet



In Missouri

The Missouri Research and Education Network (MOREnet), in collaboration with the Department of Elementary and Secondary Education and the State Library, announced a partnership with the NetSmartz Workshop to implement NetSmartz into its schools.

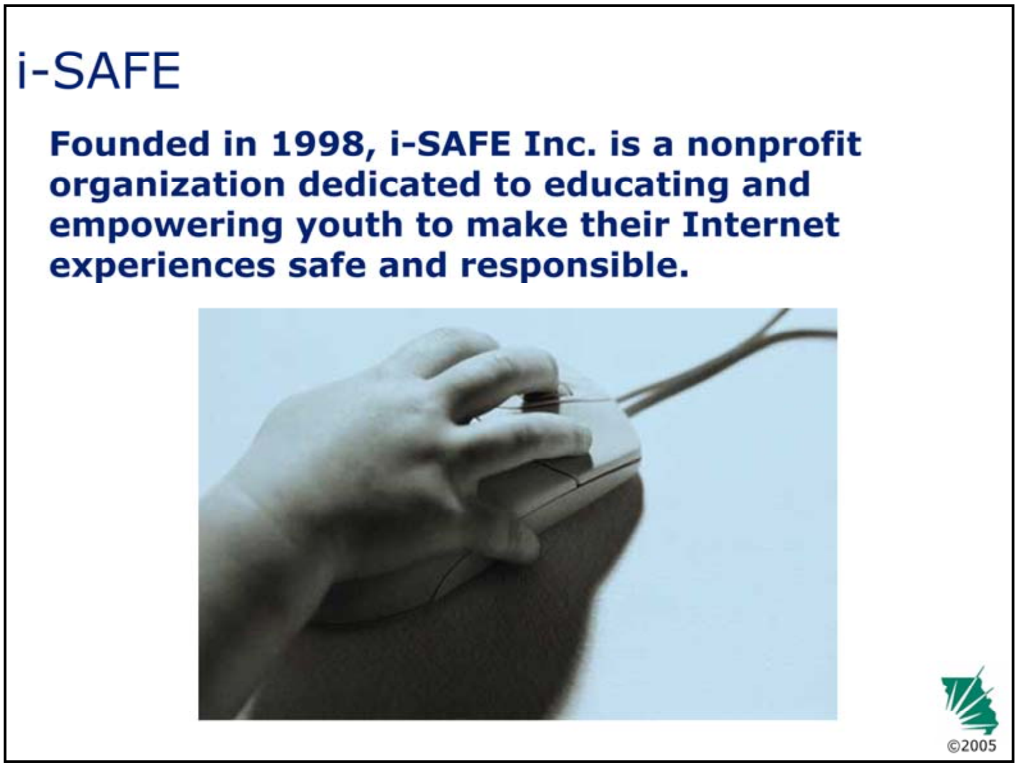
©2005

The state intranet page provides links to the downloadable version of NetSmartz. Once downloaded, this program can be used for teacher-led activities for an entire group or for students individually. Students may create their own logins and complete the activities at their own pace. Once the activities are completed, students receive a Web license and a completion certificate.

To view the downloadable version, go to: http://www.netsmartz.org/education/mo/. There are materials provided in the downloadable version that are not on the website.

Downloading the NetSmartz Program

1. Go to the state intranet site. For example, **http://www.netsmartz.org/education/mo/**. The state intranet window appears.
2. Select **All Downloads** under the **Get** link. The download information will appear.
3. Select a program for download according to the instructor and group needs. For example, under **Software** select **Netsmartz Activities.** The **Description** window appears.
4. Click on **Windows Installer** or **Macintosh Disk Image** (depending on your operating system). The **download** windows appears.
5. Follow the instructions to completely download the program.



i-SAFE

Founded in 1998, i-SAFE Inc. is a nonprofit organization dedicated to educating and empowering youth to make their Internet experiences safe and responsible.

©2005

i-SAFE Mission

Founded in 1998, i-SAFE Inc. is the leader in Internet safety education. We are a non-profit organization dedicated to educating and empowering students, parents, law enforcement, and community members to make their Internet experiences safe and responsible.

i-SAFE History

Since 2002, i-SAFE has received bipartisan recognition and support from both the Senate and the House of Representatives. Congress has awarded i-SAFE grants exceeding $14 million to expand its program in schools and communities in all 50 states and the District of Columbia. The grant is governed by a cooperative agreement with the Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice. For the school years 2004 through 2006, Congress appropriated $2 million in additional funds to implement the program in Department of Defense Education Activity (DoDEA) schools worldwide. The i-SAFE program is literally in schools around the world.

And now, through private partnerships, i-SAFE has expanded possibil-ities within other countries. The importance of Internet safety and the need for formalized classroom instruction and community awareness is an issue in all languages and countries.

i-SAFE has gone global!

i-SAFE

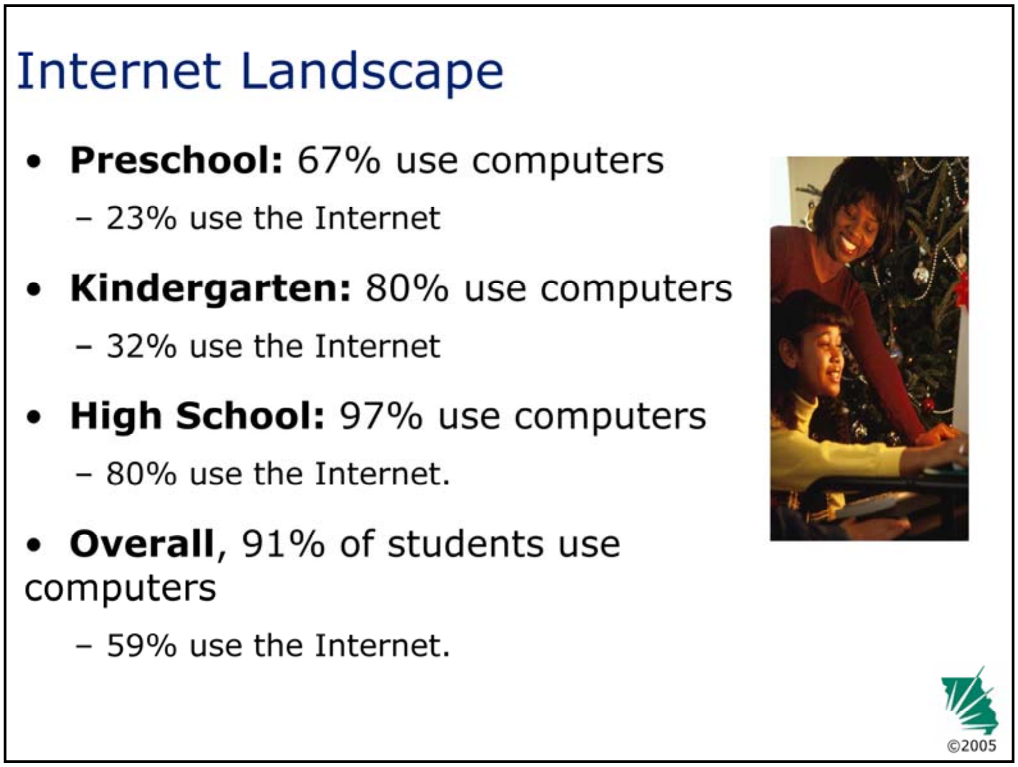
- Educate
- Empower
- Mobilize

©2005

The Internet has totally changed our lives. It has changed the way we do business. It has changed the way we communicate with one another, the way we shop and travel and educate ourselves . . . and it has changed the lives of our children, as well.

Their world is full of never-before-imagined scenarios and little concern for age or innocence. How do we, as adults, handle this issue? How do we, as adults, assume the mantle of responsibility presented to us and work to ensure the safety of our children?

i-SAFE is the global leader in Internet safety. We work around the world to educate, empower, and mobilize communities, and we do that well, as you will see here today.



Internet Landscape

- **Preschool:** 67% use computers
  - 23% use the Internet
- **Kindergarten:** 80% use computers
  - 32% use the Internet
- **High School:** 97% use computers
  - 80% use the Internet.
- **Overall**, 91% of students use computers
  - 59% use the Internet.

©2005

We are here today to learn how to empower our nation's youth to safely, responsibly, and legally use the Internet.

Let's talk first about the **need** for Internet safety education and examine i-SAFE's solution.

Statistics from the U.S. Department of Education reveal that more and more students are using computers and are online, and at a younger age.

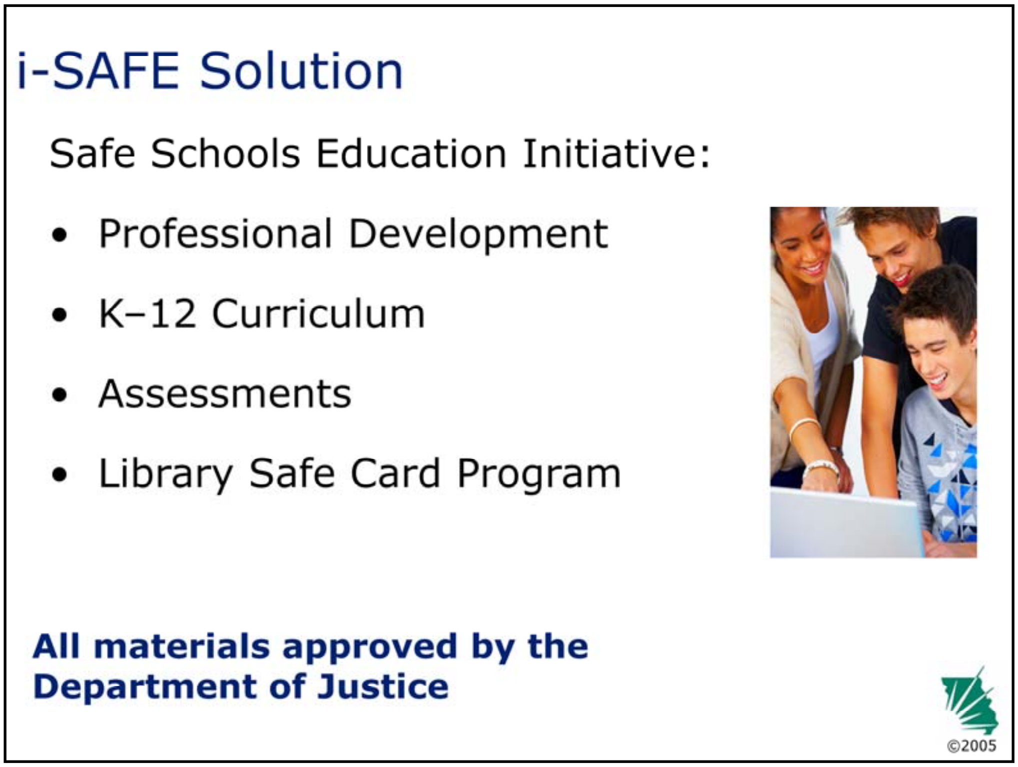
The importance of including Internet safety at every grade level cannot be overemphasized.

Overall, 91% of students use computers; 59% of those are online.

Surprisingly, this 91% includes children in preschool and kindergarten. 67% of children in nursery school use computers; 23% are online. 80% of those in kindergarten use computers.

Nearly all are computer users (97%) with 80% online.

Computers and the Internet are a fixed presence in our lives—for all age groups. And this brings its own set of issues and concerns.



i-SAFE Solution

Safe Schools Education Initiative:

- Professional Development
- K–12 Curriculum
- Assessments
- Library Safe Card Program

All materials approved by the Department of Justice

©2005

Safe Schools Education Initiative

The education components of the i-SAFE Safe Schools Education Initiative include professional development for educators and law enforcement, curriculum for students in grades K through 12, assessments, and the Library Safe Card Program.

Professional development is available three ways. 1) Premier Professional Development Program delivered via DVD 2) Facilitator-led Professional Development Program utilizing PowerPoint presentation 3) i-LEARN Online at www.isafe.org presented in online modular format

i-SAFE's curriculum includes age-appropriate, integrated teaching and learning activities for kindergarten through 8th grade, and webcasts for high-school students. Each lesson in the curriculum is designed to foster active participation between students and instructors through classroom discussions, and group and individual student activities. Each lesson is designed to extend those activities beyond the classroom—to mobilize students to take action.

All lessons and webcasts are reviewed and approved by the Department of Justice. You may view the i-SAFE "Scope and Sequence" and "Curriculum Alignment" charts at www.isafe.org.

The Library Safe Card Program includes a computer-based tutorial and quiz that serve to reinforce the concepts taught in the curriculum.

From the beginning, i-SAFE worked to assess and evaluate the program's effectiveness. We have come a long way since that first survey. During this presentation, you will see and hear our statistics, as documented by the National Assessment Center, or NAC. These numbers are invaluable to us not only by measuring our success but by guiding us as we listen to what students have to say.

Education Initiative

Attend i-SAFE's Professional Development

- Premier PDP
  - facilitated via DVD video
- PDP
  - facilitated via PowerPoint Presentation
- i-LEARN
- Virtual Training Academy

©2005

The program begins with a comprehensive professional development program to prepare educators and law enforcement to teach the curriculum.

i-SAFE uses a Train-the-Trainer approach. Through the i-SAFE professional development program, educators are certified to train other professionals to create an ever-growing network of certified trainers and classroom instructors.

1. Premier i-SAFE Professional Development Program via DVD for a group of participants

i-SAFE offers the full PDP via DVD video format that can be presented to a group of participants. For many districts, this is the best option to prepare the first tier trainers.

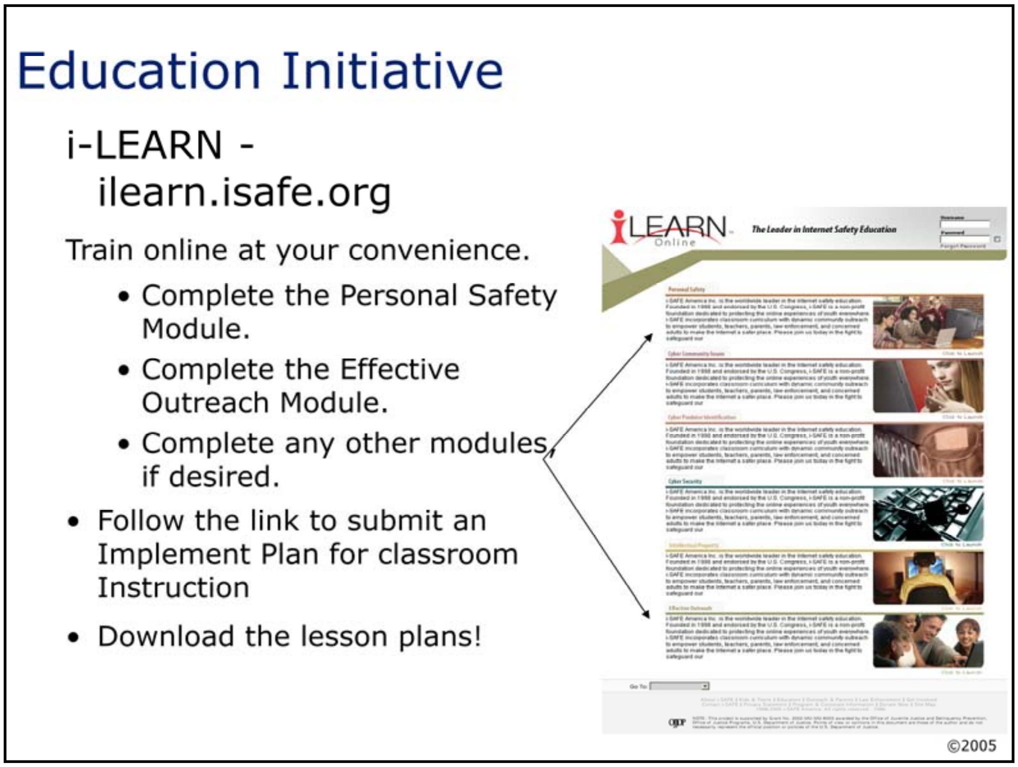
2. i-SAFE Professional Development Program facilitated by a certified trainer for a group of participants

Once you have a group of certified trainers, or even just an individual trainer, it may choose to utilize the i-SAFE four-hour scripted Professional Development Program PowerPoint Presentation, which has embedded videos to train the next group of individuals. Some trainers prefer to use the PowerPoint to facilitate their PDPs, while others prefer to continue with the video format mentioned previously. Either way leads to i-SAFE certified educators.

3. i-LEARN Online for individuals

The third option, and one that is growing in popularity, is i-LEARN Online. At http://ilearn.isafe.org, individuals can go through the modular video training at their own pace as their schedule allows. They may complete only the sections that are of interest to them or complete the entire PDP to become certified.

4. Virtual Training Academy -



Education Initiative

i-LEARN - ilearn.isafe.org

Train online at your convenience.

- Complete the Personal Safety Module.
- Complete the Effective Outreach Module.
- Complete any other modules, if desired.

- Follow the link to submit an Implement Plan for classroom Instruction
- Download the lesson plans!

©2005

The program begins with a comprehensive professional development program to prepare educators and law enforcement to teach the curriculum.

i-SAFE uses a Train-the-Trainer approach. Through the i-SAFE professional development program, educators are certified to train other professionals to create an ever-growing network of certified trainers and classroom instructors.

1. Premier i-SAFE Professional Development Program via DVD for a group of participants

i-SAFE offers the full PDP via DVD video format that can be presented to a group of participants. For many districts, this is the best option to prepare the first tier trainers.

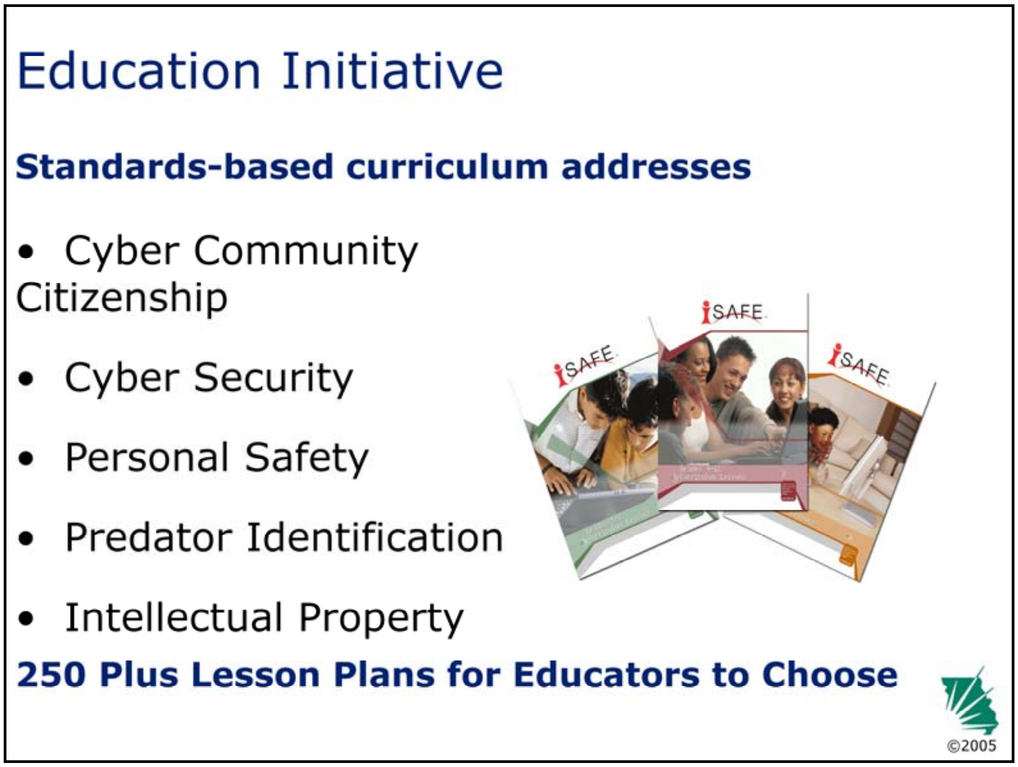
2. i-SAFE Professional Development Program facilitated by a certified trainer for a group of participants

Once you have a group of certified trainers, or even just an individual trainer, it may choose to utilize the i-SAFE four-hour scripted Professional Development Program PowerPoint Presentation, which has embedded videos to train the next group of individuals. Some trainers prefer to use the PowerPoint to facilitate their PDPs, while others prefer to continue with the video format mentioned previously. Either way leads to i-SAFE certified educators.

3. i-LEARN Online for individuals

The third option, and one that is growing in popularity, is i-LEARN Online. At http://ilearn.isafe.org, individuals can go through the modular video training at their own pace as their schedule allows. They may complete only the sections that are of interest to them or complete the entire PDP to become certified.

4. Virtual Training Academy -



Education Initiative

Standards-based curriculum addresses

- Cyber Community Citizenship
- Cyber Security
- Personal Safety
- Predator Identification
- Intellectual Property

250 Plus Lesson Plans for Educators to Choose

©2005

Education is the first step to accomplishing Internet safety, but the problem extends beyond the classroom and needs a comprehensive solution. This is where outreach comes in.

i-SAFE has three outreach campaigns—DRiVE, i-PARENT, and Operation i-SHIELD. These programs bring a comprehensive understanding of Internet safety awareness to the school, home, and community.

Students are encouraged to participate in the DRiVE Campaign—a student-powered outreach program. As i-MENTORs, students are role models who plan engaging Internet safety events and activities for their schools and communities. The program develops leadership skills, and students' involvement can fulfill community-service requirements. And, they make a difference in the lives of other students.

Parents are drawn in through the i-PARENT Campaign. Their essential involvement is encouraged with a litany of scripted, informative presentations and materials designed to educate and enable them to educate others. Parents can become part of an i-PARENT Board, joining forces to spread the word to other parents. The i-PARENT is critical in creating a framework for a safe online home and community.

Law Enforcement at the federal, state, and local levels is encouraged to partner with i-SAFE to educate teachers, community leaders, parents, and, most importantly, kids about Internet safety.

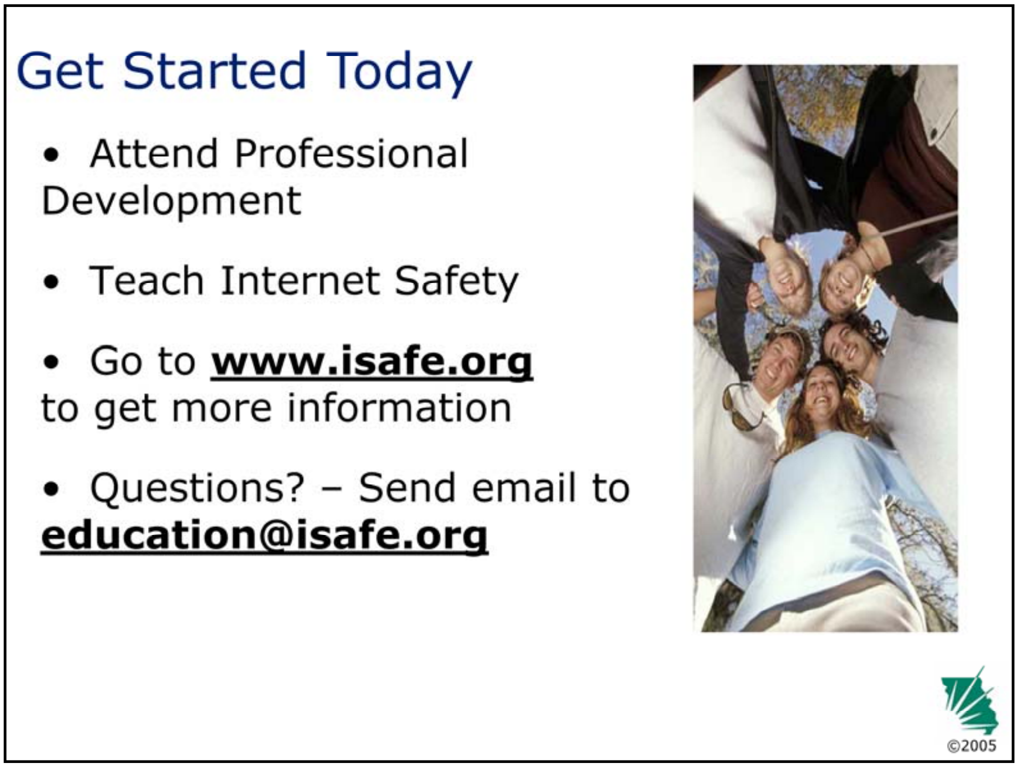
None of these campaigns can stand alone. They are integrated into the core curriculum to bring a comprehensive understanding of Internet safety awareness to the school, home, and community.

It is i-SAFE's goal to create an entire community of cyber safe citizens.

Video

http://www.isafe.org/media/SoccerGirl_Rewind.wmv

©2005

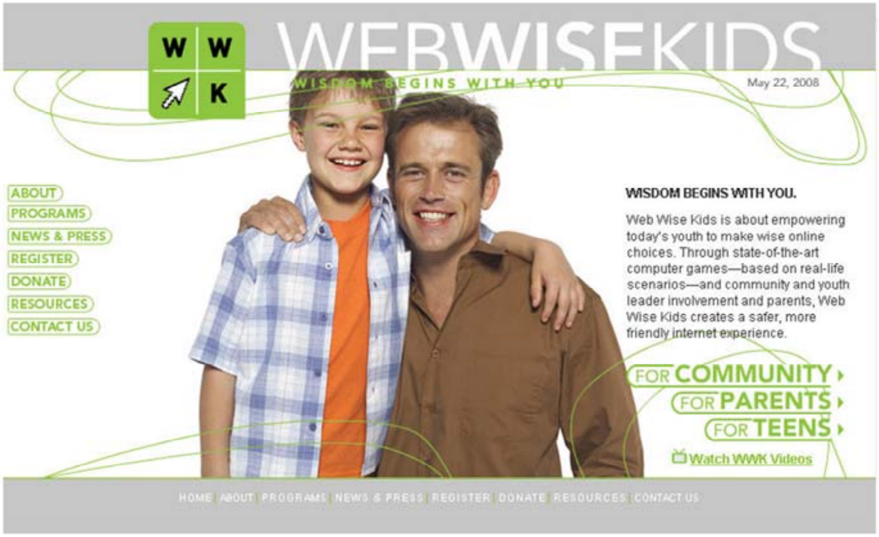


Get Started Today

- Attend Professional Development
- Teach Internet Safety
- Go to **www.isafe.org** to get more information
- Questions? – Send email to **education@isafe.org**

©2005

Web Wise Kids

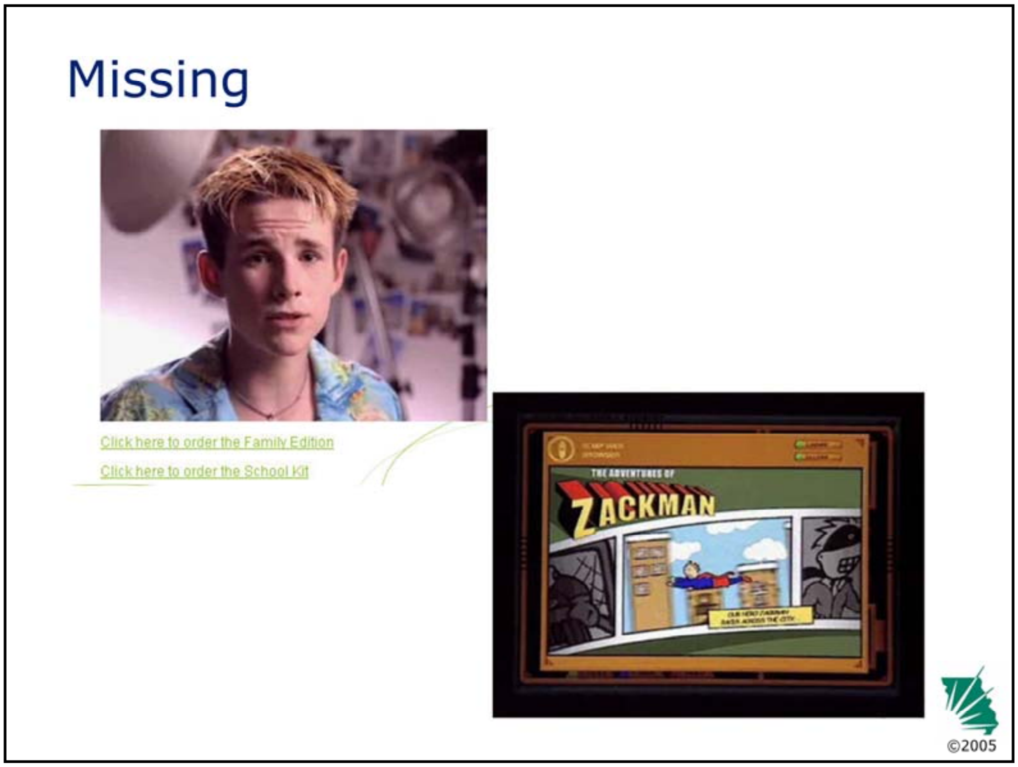


WISDOM BEGINS WITH YOU.

Web Wise Kids is about empowering today's youth to make wise online choices. Through state-of-the-art computer games—based on real-life scenarios—and community and youth leader involvement and parents, Web Wise Kids creates a safer, more friendly internet experience.

©2005

Web Wise Kids is a unique organization that offers fun, challenging and interactive simulations based on real-life criminal cases—MISSING, *Mirror Image* and *Airdogs*. Each program has been designed specifically for use with young people in classrooms and computer labs and is guaranteed to be easy to use and flexible with your classroom schedule (special versions of our programs are also available for home use). Best of all, our programs succeed at getting the message across without “another lecture.”



Missing

Click here to order the Family Edition

Click here to order the School Kit

Missing is a new kind of computer game. Half television drama and half computer game.

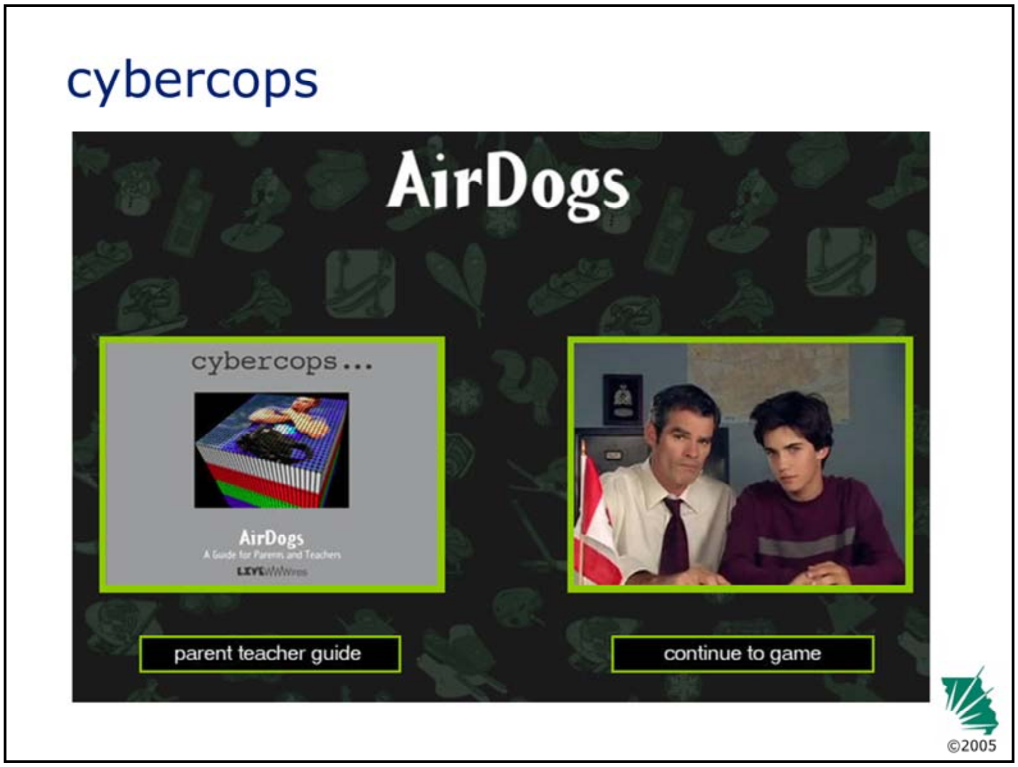
It contains as much video as a half hour television program, but it also contains games and photo animations.

MISSING tells the story of Zack, a kid in Vancouver, Canada who forms an online friendship with Fantasma. This guy is so cool - he has an online magazine about beach life in California and he sends Zack great stuff, like graphic arts and software. Little does Zack know that he is a predator. After Zach agrees to go to San Diego to be with Fantasma, players work with a detective to find and rescue Zack and arrest Fantasma.

Cybercops - Mirror Image

©2005

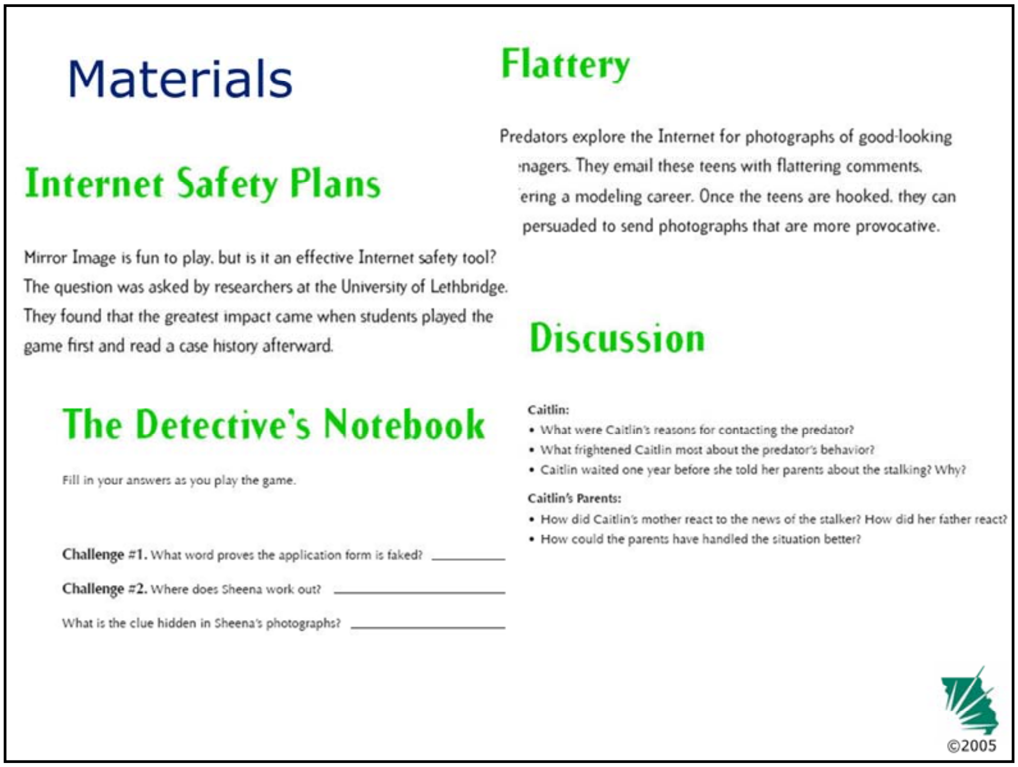
MIRROR IMAGE tells the story of teenagers Sheena and Megan, best friends who are victimized by a criminal who uses the Internet to lure young women with promises of modeling contracts and online romance. Neither of the girls realizes that hacking software has been placed on their computers during their conversations with their ‘online boyfriends.’ Soon Sheena and Megan begin to suspect that someone is stalking them in real life. Players work with a detective to track the predator and arrest him.



cybercops

©2005

AIRDOGS was designed to show teenagers that online crimes have lifelong legal and social consequences for teens and their families. In the game, Luke is a teenager who shows great promise as a snowboarder. He needs money for gear and training, so he begins to counterfeit software in his basement. Players collect data and evidence to catch Luke's boss, who is the ringleader of the operation. The message of Air Dogs is clear: theft and extortion are crimes, whether you're 16 or 60.



Materials

Flattery

Predators explore the Internet for photographs of good-looking
nagers. They email these teens with flattering comments.
ering a modeling career. Once the teens are hooked, they can
persuaded to send photographs that are more provocative.

Internet Safety Plans

Mirror Image is fun to play, but is it an effective Internet safety tool? The question was asked by researchers at the University of Lethbridge. They found that the greatest impact came when students played the game first and read a case history afterward.

Discussion

Caitlin:

- What were Caitlin's reasons for contacting the predator?
- What frightened Caitlin most about the predator's behavior?
- Caitlin waited one year before she told her parents about the stalking? Why?

Caitlin's Parents:

- How did Caitlin's mother react to the news of the stalker? How did her father react?
- How could the parents have handled the situation better?

The Detective's Notebook

Fill in your answers as you play the game.

Challenge #1. What word proves the application form is faked? __________

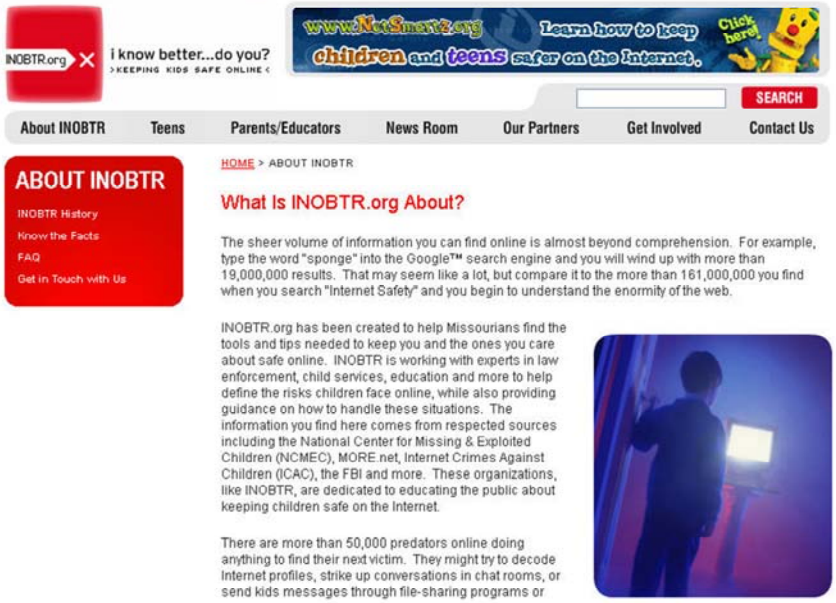
Challenge #2. Where does Sheena work out? ____________________

What is the clue hidden in Sheena's photographs? ____________________

©2005

Each game has materials to go with it to reinforce the lesson.

INOBTR.org


INOBTR.org
i know better...do you?
>KEEPING KIDS SAFE ONLINE<
www.NetSmartz.org Learn how to keep children and teens safer on the Internet. Click here!
SEARCH

About INOBTR | Teens | Parents/Educators | News Room | Our Partners | Get Involved | Contact Us

ABOUT INOBTR

- INOBTR History
- Know the Facts
- FAQ
- Get in Touch with Us

HOME > ABOUT INOBTR

What Is INOBTR.org About?

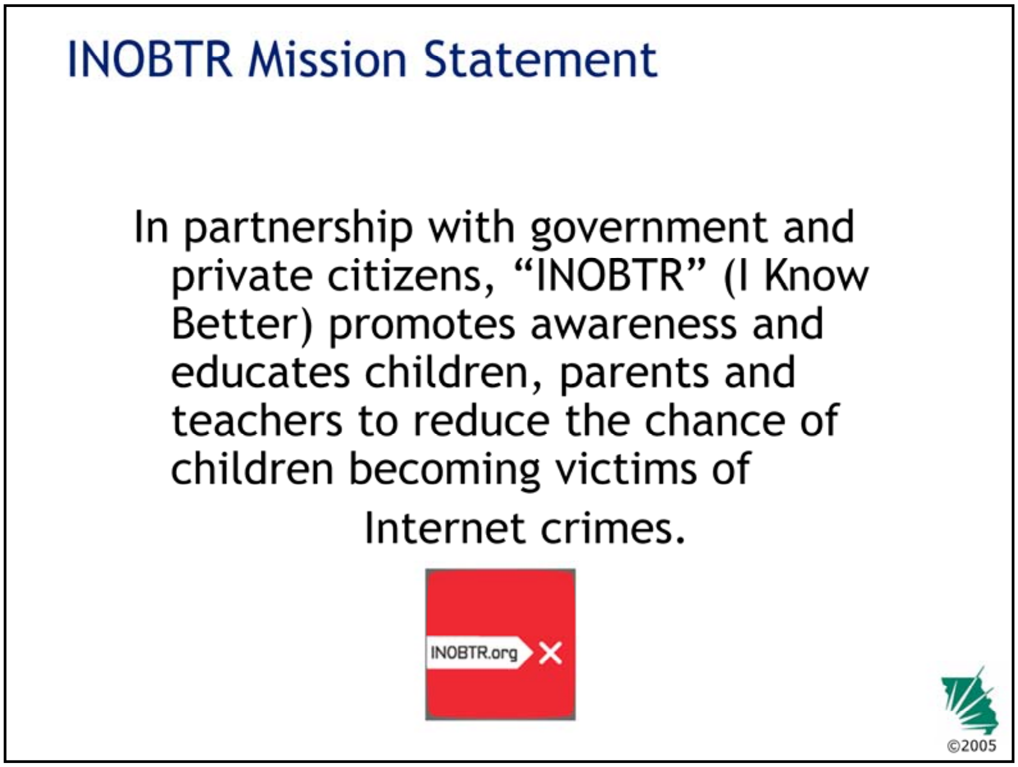
The sheer volume of information you can find online is almost beyond comprehension. For example, type the word "sponge" into the Google™ search engine and you will wind up with more than 19,000,000 results. That may seem like a lot, but compare it to the more than 161,000,000 you find when you search "Internet Safety" and you begin to understand the enormity of the web.

INOBTR.org has been created to help Missourians find the tools and tips needed to keep you and the ones you care about safe online. INOBTR is working with experts in law enforcement, child services, education and more to help define the risks children face online, while also providing guidance on how to handle these situations. The information you find here comes from respected sources including the National Center for Missing & Exploited Children (NCMEC), MORE.net, Internet Crimes Against Children (ICAC), the FBI and more. These organizations, like INOBTR, are dedicated to educating the public about keeping children safe on the Internet.

There are more than 50,000 predators online doing anything to find their next victim. They might try to decode Internet profiles, strike up conversations in chat rooms, or send kids messages through file-sharing programs or

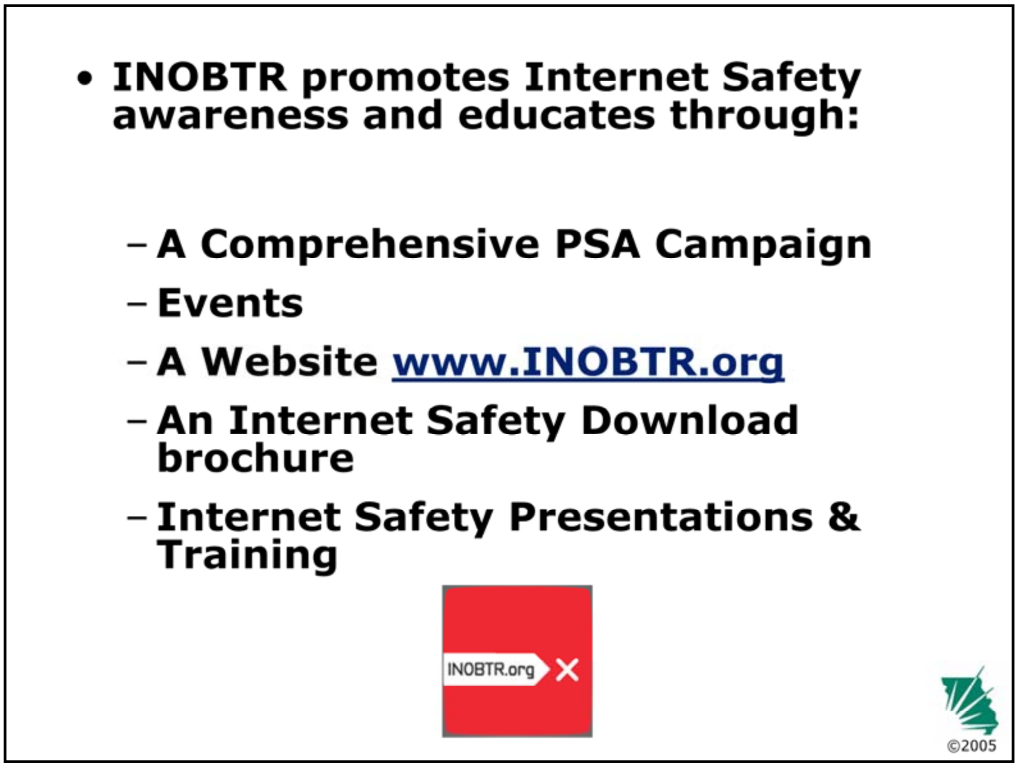
©2005

INOBTR.org has been created to help Missourians find the tools and tips needed to keep you and the ones you care about safe online. INOBTR is working with experts in law enforcement, child services, education and more to help define the risks children face online, while also providing guidance on how to handle these situations. The information you find here comes from respected sources including the National Center for Missing & Exploited Children (NCMEC), MORE.net, Internet Crimes Against Children (ICAC), the FBI and more. These organizations, like INOBTR, are dedicated to educating the public about keeping children safe on the Internet.



INOBTR Mission Statement

In partnership with government and private citizens, “INOBTR” (I Know Better) promotes awareness and educates children, parents and teachers to reduce the chance of children becoming victims of Internet crimes.



- **INOBTR promotes Internet Safety awareness and educates through:**
  - **A Comprehensive PSA Campaign**
  - **Events**
  - **A Website www.INOBTR.org**
  - **An Internet Safety Download brochure**
  - **Internet Safety Presentations & Training**

INOBTR.org
©2005

INOBTR is a 501(c)(3) non-profit organization that is Missouri's public awareness initiative to help keep kids safe online.

It is THE Internet safety resource for Missouri

Comprehensive PSA Campaign – Billboards, commercials, radio ads. Are you familiar with the Nick Lachey PSAs? Those are part of the INOBTR campaign

Events – Such as Internet Safety Night

A resourceful website at www.INOBTR.org

An Internet Safety Download resource brochure

Presentations (such as what you are taking part in today)

•This presentation doesn't begin and end with you as a participant learning more about the online safety.

•We want you to feel empowered to make a change in your home, and to share this message with your friends, family and colleagues.

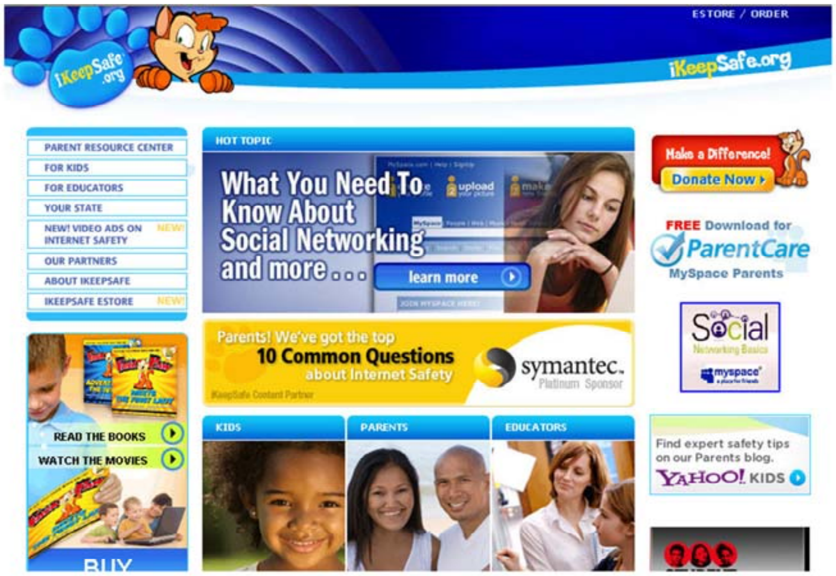
•Children are our future, and they are our responsibility.

•We must encourage everyone we know to take steps to keep children safe online.

•The safety measures we share with you today should become common practice in every home, business, and public forum.

Together, we can educate society.

IKeepSafe

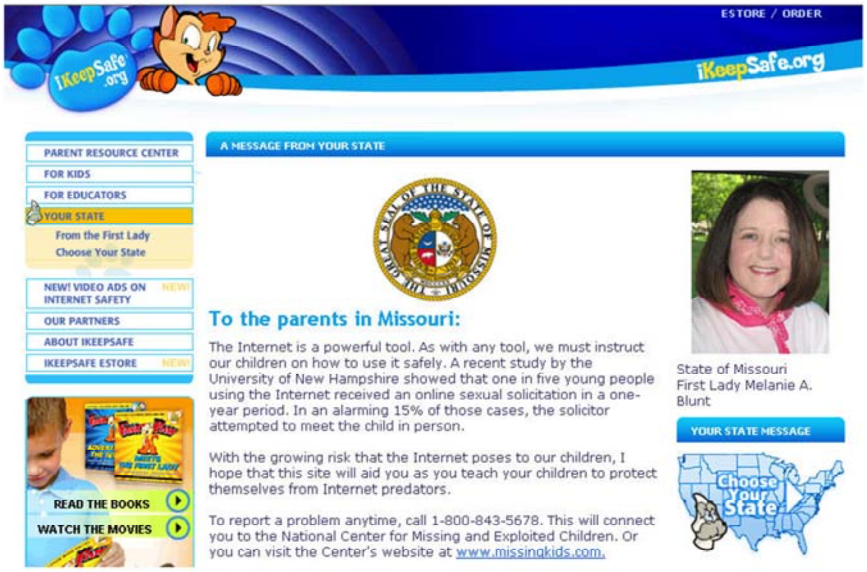


©2005

iKeepSafe® uses these unique partnerships to disseminate safety resources to families worldwide to give parents, educators, and policymakers the information and tools which empower them to teach children the safe and healthy use of technology and the Internet. iKeepSafe educational resources teach children of all ages in a fun, age-appropriate way, the basic rules of Internet safety, ethics, and the healthy use of connected technologies.

Through the storybook adventures of Internet safety icon, Faux Paw the Techno Cat®, elementary school children learn about: internet safety basics, how to handle cyber-bullying, balancing real life with screen time, the risks and dangers of downloading with educational materials, including PowerPoint® presentations, activity sheets, coloring pages, quizzes, and educational games available for free download.

IKeepSafe – Missouri



To the parents in Missouri:

The Internet is a powerful tool. As with any tool, we must instruct our children on how to use it safely. A recent study by the University of New Hampshire showed that one in five young people using the Internet received an online sexual solicitation in a one-year period. In an alarming 15% of those cases, the solicitor attempted to meet the child in person.

With the growing risk that the Internet poses to our children, I hope that this site will aid you as you teach your children to protect themselves from Internet predators.

To report a problem anytime, call 1-800-843-5678. This will connect you to the National Center for Missing and Exploited Children. Or you can visit the Center's website at www.missingkids.com.

State of Missouri
First Lady Melanie A. Blunt

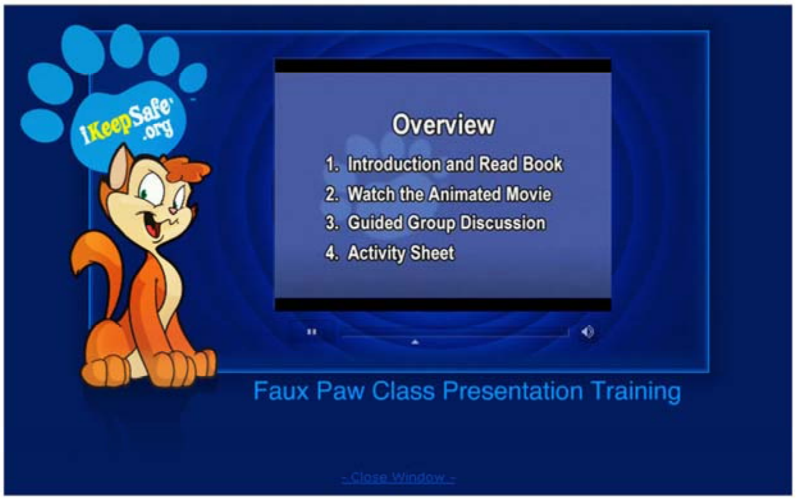
©2005

The Internet Keep Safe Coalition is a broad partnership of governors and/or first spouses, attorneys general, public health and educational professionals, law enforcement, and industry leaders working together for the health and safety of youth online. iKeepSafe® uses these unique partnerships to disseminate safety resources to families worldwide.

Ikeepsafe – Activities

©2005

IKeepSafe – Presenter training



Overview

1. Introduction and Read Book
2. Watch the Animated Movie
3. Guided Group Discussion
4. Activity Sheet

Faux Paw Class Presentation Training

- Close Window -

©2005

Simple step-by-step video training for teachers and volunteers demonstrating suggested methods to conduct the "Class Presentations". Each book in the Faux Paw series is highlighted followed by a 4-part classroom demonstration of the "Class Presentation".

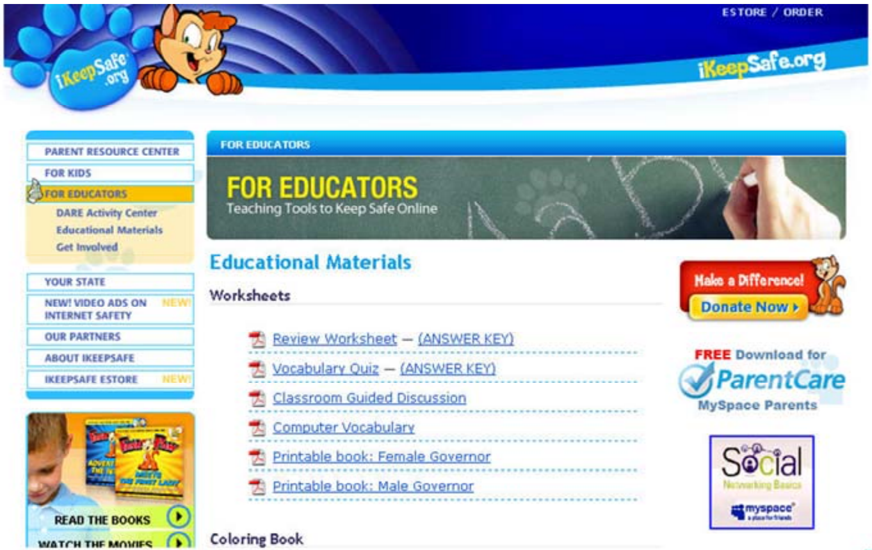
Resources for Teens

©2005

Comcast’s Emmy award-winning “Student Voices” on cyber-bullying

‘Tween and teen video presentations and tutorials

IKeepSafe – Educator Resources



PARENT RESOURCE CENTER
FOR KIDS
FOR EDUCATORS
DARE Activity Center
Educational Materials
Get Involved
YOUR STATE
NEW! VIDEO ADS ON INTERNET SAFETY NEW!
OUR PARTNERS
ABOUT IKEEPSAFE
IKEEPSAFE ESTORE NEW!

READ THE BOOKS
WATCH THE MOVIES

FOR EDUCATORS

FOR EDUCATORS
Teaching Tools to Keep Safe Online

Educational Materials

Worksheets

- Review Worksheet — (ANSWER KEY)
- Vocabulary Quiz — (ANSWER KEY)
- Classroom Guided Discussion
- Computer Vocabulary
- Printable book: Female Governor
- Printable book: Male Governor

Coloring Book

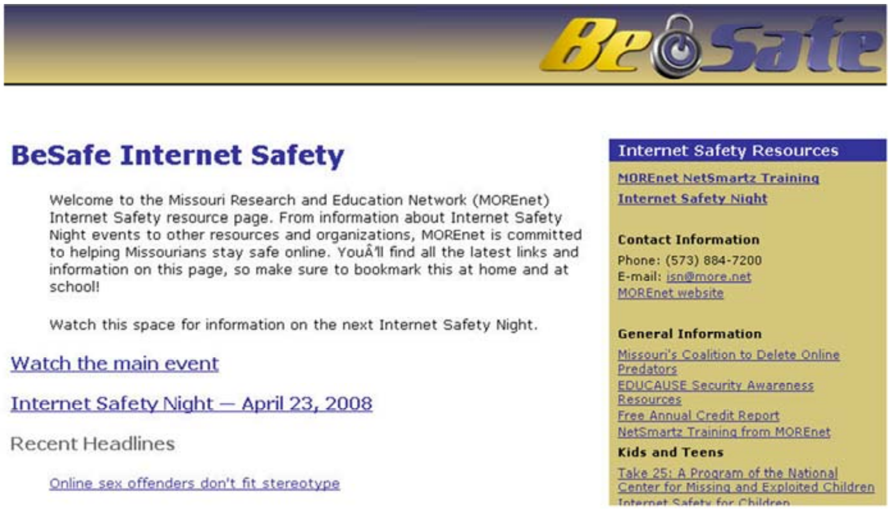
Make a Difference!
Donate Now

FREE Download for
ParentCare
MySpace Parents

Social
Networking Basics
myspace

http://www.ikeepsafe.org/iksc_educators/educational-materials.php

Besafe



BeSafe Internet Safety

Welcome to the Missouri Research and Education Network (MOREnet) Internet Safety resource page. From information about Internet Safety Night events to other resources and organizations, MOREnet is committed to helping Missourians stay safe online. YouÂ'll find all the latest links and information on this page, so make sure to bookmark this at home and at school!

Watch this space for information on the next Internet Safety Night.

Watch the main event

Internet Safety Night — April 23, 2008

Recent Headlines

Online sex offenders don't fit stereotype

Internet Safety Resources

MOREnet NetSmartz Training

Internet Safety Night

Contact Information

Phone: (573) 884-7200
E-mail: isn@more.net
MOREnet website

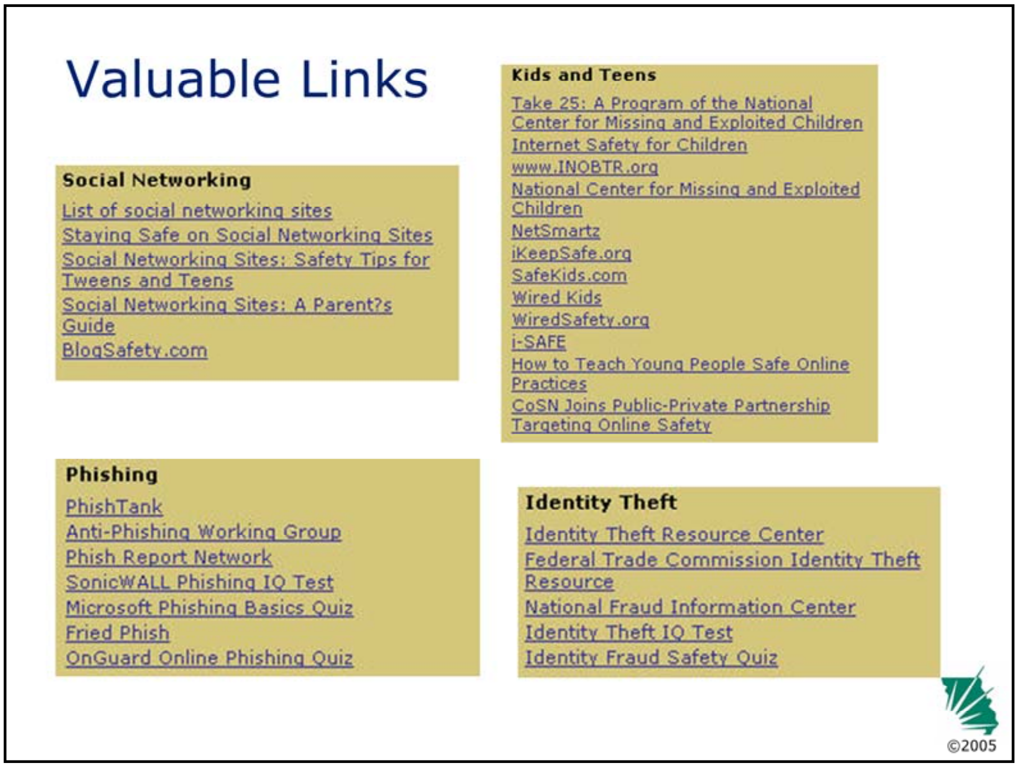
General Information

Missouri's Coalition to Delete Online Predators
EDUCAUSE Security Awareness Resources
Free Annual Credit Report
NetSmartz Training from MOREnet

Kids and Teens

Take 25: A Program of the National Center for Missing and Exploited Children
Internet Safety for Children

Besafe is the Missouri Research and Education Network (MOREnet) Internet Safety resource page. From information about Internet Safety Night events to other resources and organizations, MOREnet is committed to helping Missourians stay safe online. You'll find all the latest links and information on this page.



Valuable Links

Social Networking

- List of social networking sites
- Staying Safe on Social Networking Sites
- Social Networking Sites: Safety Tips for Tweens and Teens
- Social Networking Sites: A Parent?s Guide
- BlogSafety.com

Kids and Teens

- Take 25: A Program of the National Center for Missing and Exploited Children
- Internet Safety for Children
- www.INOBTR.org
- National Center for Missing and Exploited Children
- NetSmartz
- iKeepSafe.org
- SafeKids.com
- Wired Kids
- WiredSafety.org
- i-SAFE
- How to Teach Young People Safe Online Practices
- CoSN Joins Public-Private Partnership Targeting Online Safety

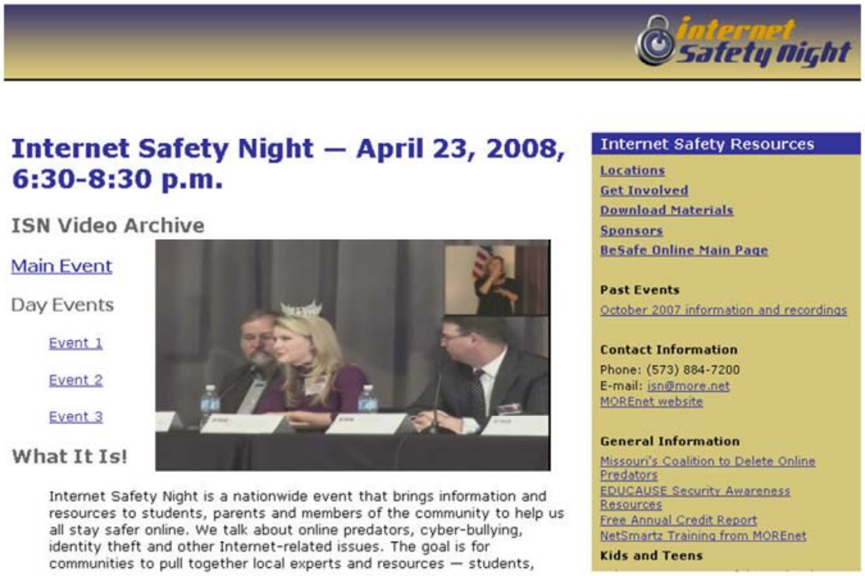
Phishing

- PhishTank
- Anti-Phishing Working Group
- Phish Report Network
- SonicWALL Phishing IQ Test
- Microsoft Phishing Basics Quiz
- Fried Phish
- OnGuard Online Phishing Quiz

Identity Theft

- Identity Theft Resource Center
- Federal Trade Commission Identity Theft Resource
- National Fraud Information Center
- Identity Theft IQ Test
- Identity Fraud Safety Quiz

Internet Safety Night



Internet Safety Night — April 23, 2008, 6:30-8:30 p.m.

ISN Video Archive

Main Event

Day Events

- Event 1
- Event 2
- Event 3

What It Is!

Internet Safety Night is a nationwide event that brings information and resources to students, parents and members of the community to help us all stay safer online. We talk about online predators, cyber-bullying, identity theft and other Internet-related issues. The goal is for communities to pull together local experts and resources — students,

Internet Safety Resources

Locations
Get Involved
Download Materials
Sponsors
BeSafe Online Main Page

Past Events

October 2007 information and recordings

Contact Information

Phone: (573) 884-7200
E-mail: isn@more.net
MOREnet website

General Information

Missouri's Coalition to Delete Online Predators
EDUCAUSE Security Awareness Resources
Free Annual Credit Report
NetSmartz Training from MOREnet

Kids and Teens

Internet Safety Night is a nationwide event that brings information and resources to students, parents and members of the community to help us all stay safer online. We talk about online predators, cyber-bullying, identity theft and other Internet-related issues. The goal is for communities to pull together local experts and resources — students, parents, teachers, law enforcement and community members — to begin a discussion about the importance of Internet safety. These local discussions, occurring simultaneously all around the country, then connect to the national host site in Columbia, Mo. for the featured speakers and other resources and tools that families can use to stay safe. Participants at any of the local events can see, hear, ask and answer questions in real time with participants at any of the other sites!