Instructor's Guide

CYBERSENSE

CyberSafety • CyberSecurity • CyberEthics

Introduction

This Instructor's Guide provides information to help you get the most out of the three-part series *CyberSense*. The contents of the guide will allow you to prepare your students before using the series and to present follow-up activities to reinforce its key learning points.

Taking a no-nonsense, peer-based approach, this three-part series raises teen awareness of the threats that Internet users face. Personal, financial, and career-related risks become clear through conversations with young people and interviews with computer experts—including Ron Teixeira, Executive Director of the National Cyber Safety Association; Dean Daley, an experienced computer systems analyst; and Marsali Hancock of the Internet Keep Safe Coalition. Students will gain a solid understanding of best practices and rules of online conduct, so that they can navigate potential Internet perils before trouble occurs. Through this program, students expand their Internet savvy, learn what behaviors and choices to avoid, consider more appropriate actions to take to result in positive consequences, and become more aware, thoughtful online participants. *CyberSense* helps guide students down a path of starting to make appropriate choices while utilizing the Internet, a skill set they can then expand to a wider set of online behaviors and decisions.

Learning Objectives

After watching this three-part series, students will be able to:

- Understand and identify behaviors and external factors that can place them at risk when using the Internet in various capacities.
- Identify some of the main categories of potential online problem areas.
- Understand the specific challenges that each online problem area poses.
- Identify strategies that can be used to help circumvent potentially dangerous online situations before trouble happens.

National Educational Standards

Technology Standards

This program correlates with the National Educational Technology Standards from the National Education Technology Standards Project. The content has been aligned with the following educational standards and benchmarks from this organization.

- Students understand the ethical, cultural, and societal issues related to technology.
- Students practice responsible use of technology systems, information, and software.
- Students develop positive attitudes toward technology uses that support lifelong learning, collaboration, personal pursuits, and productivity.

The activities in this instructor's guide were created in compliance with the following National Education Technology Standards from the National Education Technology Standards Project.

- Technology Productivity Tools Students use telecommunications to collaborate, publish, and interact with peers, experts, and other audiences.
- Social, Ethical, and Human Issues Students understand the ethical, cultural, and societal issues related to technology.
- Social, Ethical, and Human Issues Students practice responsible use of technology systems, information, and software.
- Technology Communication Tools Students use technology to locate, evaluate, and collect information from a variety of sources.

The National Education Technology Standards reprinted with permission from the International Society for Technology in Education.

English Language Arts Standards

The activities in this Teacher's Guide were created in compliance with the following National Standards for the English Language Arts from the National Council of Teachers of English.

- Writing Gathers and uses information for research purposes.
- Writing Uses strategies to adapt writing for different purposes (e.g., to explain, inform, analyze, entertain, reflect, persuade)
- Reading Uses discussions with peers as a way of understanding information.
- Media Understands the characteristics and components of the media
- Listening and Speaking Uses listening and speaking strategies for different purposes.

Standards for the English Language Arts, by the International Reading Association and the National Council of Teachers of English, Copyright 1996 by the International Reading Association and the National Council of Teachers of English. Reprinted with permission.

Program Overview

CyberSense is divided into three video components: *CyberSafety, CyberSecurity,* and *CyberEthics.* Each addresses potential trouble spots students may encounter while online, and how they should best avoid or deal with these situations. Students may not realize all of the challenges they might encounter while utilizing the Internet, and thus be unprepared to successfully navigate these problems. After viewing the three sections of this program, students will have more knowledge of what they might experience on the Internet, and more confidence in their ability to handle these problems.

CyberSafety: What harm could come from sitting leisurely at the computer, chatting with online pals? Unfortunately, many young people who spend hours in chat rooms or post sensitive information on the Internet have little or no idea of the risks involved. This program warns students about how vulnerable they are whenever they venture into the cyber realm—even when they think they're among "friends." Explaining how to take precautions in chat rooms, on social networking sites, and anywhere that predators lurk, the program strongly advises against physically meeting any online acquaintance and emphasizes that parents or guardians must be involved in such meetings. Commentary from experts and questions from peers reinforce the notion of an irreversible virtual footprint—a trail that all Internet users leave which can be used against them.

CyberSecurity: The Internet offers vast possibilities for learning, making a living, and having fun —but it can also destroy reputations, empty bank accounts, and ruin lives. This program cautions students about potential hazards to their computers—not to mention their careers, finances, and futures—that exist online. Highlighting the importance of setting up a firewall and keeping one's operating system up-to-date, the program provides straightforward advice about protecting against hackers, viruses, Trojan horses, spyware, adware, phishing emails, and other high-tech threats. Each concept is defined in user-friendly terms. More basic but equally vital steps like maintaining multiple passwords and not sharing personal information are also discussed. Commentary from experts, as well as questions from peers about the details of computer safeguards, will help students increase their online security.

CyberEthics: Most people learn traditional standards of behavior and respect for others by the time they are teenagers—but many don't realize that those rules are just as valid in cyberspace. This program helps students take the high road on the information superhighway and avoid the temptations of the fast lane, pointing the way toward an ethically sound Internet presence and lifestyle. Guidelines for the use of intellectual property are featured, with emphasis on the consequences of illegal downloading, copyright infringement, and plagiarism. Pornography, gaming sites, chat rooms, and online social networks are also discussed, helping viewers steer clear of antisocial and abusive activities, especially cyber-bullying. Commentary from experts, as well as questions from peers who are confused about the fine points of cyber legality, serves to clarify central ethical principles.

Fast Facts

- An important first step in Internet safety is to secure your computer with a firewall.

- Be careful when you download free games or other software—you might actually be downloading a virus. A virus can cause damage to your computer files or disrupt your computer system.

- Never share your Internet passwords, even with your close friends. Not only could someone log in as you and access your personal information, but he or she could also commit illegal or unethical activities in your name.

- Exercise caution when making purchases online. Verify company policies for payment, returns, and shipping, and always keep records of the transaction.

- Just because you see something on the Web doesn't mean it is true! Remember, people can post whatever they want online, regardless of the actual facts.

- Copyright protection applies on the Internet, and not just to books and other items in print. If you download music, games, or movies without appropriate permission or payment, you are actually stealing and may be subject to legal penalties.

- When posting your personal information online, be sure to check the privacy settings on the site you are using. Never post information such as your home address, and consider not posting photos of yourself.

- Remember that when you post something online, it never really goes away—even if you delete it. Keep that in mind whenever you post something on the Internet, and especially when you consider posting photos.

- It's possible to purchase or copy full school papers online. Although this might be a tempting way to get out of researching and writing a paper, don't make this mistake. Turning in a copied paper is plagiarism, and, depending on your school's academic integrity policy, it might mean you receiving a failing grade for the paper or class. There are electronic tools that help teachers discover this type of plagiarism (as well as their common sense in detecting different writing styles), so it's very likely you will be caught.

Vocabulary Terms

cyberbullying: Harassment, taunting, and teasing committed online, such as in chat rooms or by posting inappropriate or false information or images of someone.

firewall: Internet security software and/or hardware that protects your computer against unauthorized access.

hacking: Entering another user's computer without permission and undertaking activities such as stealing personal information or crashing the system; the digital equivalent of breaking and entering.

intellectual property: Property of the mind including ideas, inventions, and creations such as art and music.

PayPal: Third party vendor online that allows users to securely send and receive online payments via bank account or credit card.

phishing: Tricking users into revealing personal information such as passwords and bank account numbers by way of emails purporting to be from actual companies; users are directed to a bogus Web site and asked to input sensitive information which can then be used in identity theft.

plagiarism: Copying or using someone else's work and taking credit for it without acknowledging the real author. Plagiarism can occur online when students copy or buy academic papers and turn them in as original work, or when they copy passages from online and paste it into their own work.

spyware: Malicious software that enters a computer and tracks or gathers personal information on that computer without the knowledge of that computer's user, often for marketing purposes. Spyware can also be responsible for pop-up ads and even identity theft.

Trojan horse: Computer program that appears to be a harmless or helpful application (such as a game) but actually causes damage to a computer once downloaded.

virtual (or digital) footprint: Information about yourself that you leave online through postings and photographs. Even if you delete something, it remains online in some capacity—don't forget that every action you take online is permanent.

virus: Malicious software that enters a computer and negatively affects that computer's ability to run correctly.

Pre-Program Discussion Questions

1. How do you use the Internet? When do you go online, and for how long? What are your favorite things to do online?

2. Have you ever experienced a dangerous or uncomfortable situation online? What happened? What did you do in response? How did the situation end?

3. What are some of the Web sites you enjoy using?

4. Have your parents or teachers ever talked to you about online safety or appropriate behavior on the Internet? What did they say? Did you take them seriously? Why or why not?

5. Why is the Internet useful? Why is it fun? How might it be dangerous or damaging?

Post-Program Discussion Questions

1. What were you surprised to learn from watching this program? What did you hear or see that you already knew? Have you ever been in any of the negative situations described in this program? What happened?

2. If you were making a video about Internet safety and appropriate behavior, what additional information would you include that was not in this program? What hypothetical scenarios might you use to illustrate these points?

3. How can you commit copyright violation while online? Why are copyrights important? Do you think you should respect or pay attention to copyrights while online? Why or why not?

4. What are some examples of programs or behaviors that can damage your computer or computer files? How might you be exposed to these dangers? How can you avoid these problems?

5. If you had to give a younger sibling or cousin advice about behaving appropriately and safely while online, what would you say? What specific examples might you give to emphasize your advice?

Individual Student Projects

Creative Writing

Students may have had troubling experiences while surfing the Internet, yet be reluctant to share details with the rest of the class. Through a creative writing exercise, students can voice concerns without drawing publicly on personal experience.

Let the class know that they will be developing and writing realistic fictional stories featuring a teen protagonist facing cybersense issues. Students will detail a situation, and the choices the protagonist ultimately makes—whether those choices are advisable or not. Sample situations might include:

- Striking up a correspondence with someone who then begins to seem creepy, or who invites you to meet in person
- Participating in (or being a victim of) cyberbullying
- Accidentally downloading a virus—and then passing it along to your friends
- Accidentally encountering a pornographic Web site
- Being tempted to illegally download music or a movie
- Deciding whether or not to block-copy from Wikipedia for use in a research paper

Invite students to read their stories to the class. At the end of each story, conduct a discussion on whether or not the protagonist made the best choice, and share other possible solutions and ideas.

Research and Writing

Students who have used the Internet for years without incident might write off the *CyberSense* programs as being unlikely or unrealistic. To this end, assign a research paper on Internet safety that will include statistics on young people's experiences online, identity theft and copyright infringement, cyberbullying, computer viruses, and predators. A good place to start is http://www.protectkids.org/statistics.htm. Remind students to be aware of cyber-plagiarism as they write their papers—if they quote an online source they need to give full credit, and papers must be written in their own words.

Have students present their papers to the rest of the class. What are some common themes? What information was surprising? Ultimately, why is Internet safety education and awareness important?

Other Ideas for Individual Activities

Have students ...

- Compile a list of appropriate and useful Web sites for younger students.

- Create a poster, Web page, film, song, or written guide about keeping your computer safe; include information on firewalls and other ways to avoid viruses, adware, spyware, etc.

- Create a poster, Web page, film, song, or written guide on intellectual property as it relates to the Web.

- Investigate Teenangels (www.teenangels.com), a group of teens trained to run programs and give presentations in schools and elsewhere on cyber safety. Would you be interested in joining or forming a local chapter?

Group Activities

Advice Column

Have the class take a minute to think about an Internet-related issue that is unclear to them, and then record it as a question at the top of a loose sheet of paper. Then divide students into groups of three or four. Students should pass their written inquiry to the person to their right. The student who receives the question will write their answer to it (or best guess!) as well as their reasoning for that response. After answering, students fold up the paper to cover their answer but leave the original question and rest of the blank paper showing. Groups should continue passing, answering, and folding until the question reaches the original author.

One at a time around the circle, authors should share their question and the responses received. Groups should debate the answers—which makes the most sense? Which is the most creative? Finally, ask groups to determine and then share with the rest of the class the question they found most interesting, most difficult to answer, or most hotly debated.

Stopping the Cyberbully

For all the enjoyment that social networking sites, email, and chat programs bring students, they can also deliver embarrassment, anger, and frustration when they are used to bully and harass others.

Ask students to define cyberbullying in their own words, and to pose some questions. Why does cyberbullying happen? Who might become a cyberbully, and who might become a victim? Why do some people allow cyberbullying to happen, even when they are not taking part in it themselves? How is cyberbullying like face-to-face bullying, and how is it different? Why is it harmful, and how can it be stopped?

Break students into small groups and have them write short skits that address and illustrate the questions above. Make sure students work facts and statistics into their presentations, either in the body of the skit, or before or after as "commentary."

Other Ideas for Group Activities

Have students ...

- Create a poster, Web page, film, song, or written guide to Internet safety either for peers or directed at younger students.

- Design and play a trivia game using facts and information on cyber safety, cyber security, and cyber ethics.

- Answer the question "Is It Wrong to Steal From Rock Stars?" via a formal debate on the legality and ethics of downloading music on peer-to-peer sharing sites.

Internet Activities

Developing a Good Profile

Social networking sites and personal Web pages are a standard part of today's Internet experience, as is communicating with new friends who share similar interests. But making public too much personal information can be dangerous. How can students create profiles and Web sites that reflect who they really are without making themselves vulnerable to predators?

Have students work together to build a mock profile for a social networking site. First, on paper, create a hypothetical teen, including a name, address, age, a list of abilities, interests, likes and dislikes, and personal style.

Next, students should build a profile that accurately reflects the personality they have created without giving away too much private information. For instance, instead of including personal photos of the student, the profile might include photos the student has taken or art he/she has created. Instead of stating that a student is attending a particular upcoming concert, the profile might have a picture of a favorite band or samples of the band's music. (Students should also remember to respect the copyright and usage policies of material they find online!)

Ask the class if the profile they built is effective. Did it get across the nuances of a unique personality without revealing a true identity to all of cyberspace?

Copyright Questions

Copyright infringement is a hot topic on the Internet today. You may get away with illegally downloading, but you are taking a risk. For one, there are strict penalties should you be caught and prosecuted. Second, some of the programs that facilitate peer-to-peer sharing of files can allow other people access to personal files on your computer. Finally, there are ethical implications to taking what does not belong to you.

Ask students to explore at least four different sites where users could download movies or music. Together, students should determine whether downloading files from these sites is actually safe and legal. They might find this information by reading the terms of use, by debating and using common sense (if an album just released in the stores yesterday is free online, is it likely that downloading it is legal?), and by researching the topic further (via recent court cases, newspaper articles, and record company Web sites, for instance). Students might also research the penalties for illegally downloading and using copyrighted files.

Have the class reflect on the information they uncovered. Have they inadvertently downloaded illegally? Have they known what they were doing was wrong but done it anyway? Students may not want to admit to this behavior, so you may have them reflect silently or write in journals. As a class, research some online sites where it is definitely legal to purchase music or download files.

Other Ideas for Internet Activities

- Have students use online resources to compile a list of books, articles, and links related to either Internet safety, security, or ethics. They should include Web sites where it is possible to report cases of cyberabuse (stalking, hacking, identity theft, child pornography, etc.). You might have a media specialist guide this exercise to emphasize strong online research skills.

- With students, examine the types of filter/blocking programs available (often used by schools and public libraries, among other uses). These programs prevent students and others from visiting certain types of Web sites. Do these programs work? Should they be used? In what situations?

- Have students conduct research into some of the negative consequences of online gambling or gaming. Why can these pursuits be enjoyable? How can they be dangerous or a cause for concern?

- As a class, start a blog about Internet safety and ethics. Ask all students in your class to contribute in some way, and invite other students (either other classes or peers at other schools) to participate.

- Collect examples of phishing emails that purport to be from eBay, Bank of America, etc.; include tips on how to tell these emails are not legit.

Assessment Questions

1. What is a Trojan horse?
   a) An anti-virus software program
   b) Malicious software that disguises itself as a harmless program
   c) Software that infects a computer and displays advertisements
   d) A type of copyright policy

2. How can you avoid or stop cyberbullying?
   a) Ignore the bullying and do not participate
   b) Report the problem to a parent or teacher
   c) Report the abuse at www.wiredsafety.org
   d) All of the above

3. What is a virtual or digital footprint?

4. What is intellectual property?
   a) Online real estate listings
   b) Spyware
   c) Ideas, inventions, and creations such as art
   d) Plagiarism

5. Why are anti-virus software programs and firewalls useful?

6. If you had to give a friend three pieces of advice about appropriate Internet behavior, what would they be, and why?

7. Define hacking.

8. What is malware?
   a) Malicious software designed to damage a computer system
   b) A teen social networking site
   c) A hotline to contact about cyberbullying
   d) None of the above

9. How might your behavior on the Internet now affect you in the future?

10. How can the Internet simultaneously be a great place for research, friendships, and shopping, and a dangerous place with many potential trouble spots?

Assessment Questions Answer Key

1. What is a Trojan horse?
   a) An anti-virus software program
   b) Malicious software that disguises itself as a harmless program
   c) Software that infects a computer and displays advertisements
   d) A type of copyright policy
      Answer: (b) malicious software that disguises itself as a harmless program
      Always exercise caution when downloading unfamiliar programs—they could seriously harm your computer. When in doubt, don't download.

2. How can you avoid or stop cyberbullying?
   a) Ignore the bullying and do not participate
   b) Report the problem to a parent or teacher
   c) Report the abuse at www.wiredsafety.org
   d) All of the above
      Answer: (d) All of the above
      Do not participate in cyberbullying in any capacity —whether by starting it or responding to it. Try to stop cyberbullying before it becomes a real problem by following the tips in CyberEthics.

3. What is a virtual or digital footprint?
      Answer: A virtual or digital footprint is the personal information you leave about yourself on the Internet through your posts, online conversations, and online photos. Remember that anything you post online never really goes away. Make sure you are being safe and aware, and that your cyber footprint accurately reflects the person you want to be—and that you want potential employers to see.

4. What is intellectual property?
   a) Online real estate listings
   b) Spyware
   c) Ideas, inventions, and creations such as art
   d) Plagiarism
      Answer: c) ideas, inventions, and creations such as art
      Avoid plagiarizing or stealing the intellectual property of others. Always get permission or make the appropriate payment for use of intellectual property, and give credit to the original author/developer.

5. Why are anti-virus software programs and firewalls useful?

   Answer: Anti-virus software programs and firewalls prevent authorized and possibly damaging access to your computer. They help prevent hackers from accessing your files, as well as assist in keeping malicious software from acting on your computer systems. Always keep your virus protection active and up-to-date.

6. If you had to give a friend three pieces of advice about appropriate Internet behavior, what would they be, and why?

   Answer: Students might write about protecting personal information, keeping computers up- to-date with anti-virus software, avoiding and reporting cyberbullying, or leaving an appropriate cyber footprint, among other answers. Remind students that if they are thinking about taking part in questionable online activity, they should think about what advice they might give a friend in the same situation.

7. Define hacking.

   Answer: Hacking involves breaking into another person's computer without his or her permission. Once in, the hacker might steal personal information or corrupt system files. Students should install a firewall to help prevent hackers from accessing their computers.

8. What is malware?

   a) Malicious software designed to damage a computer system
   b) A teen social networking site
   c) A hotline to contact about cyberbullying
   d) None of the above

   Answer: a) malicious software designed to damage a computer system
   Firewalls, anti-virus software, and careful consideration and assessment of programs you choose to download can help prevent malware on your computer.

9. How might your behavior on the Internet now affect you in the future?

   Answers will depend on individual students. Encourage students to share their thoughts in oral presentations, or, if there are differing opinions in your class, in an organized debate.

10. How can the Internet simultaneously be a great place for research, friendships, and shopping, and a dangerous place with many potential trouble spots?

    Answers will depend on individual students. Encourage students to share their thoughts in oral presentations, or, if there are differing opinions in your class, in an organized debate.

Additional Resources

i-SAFE Inc.: The Leader in Internet Safety Education
www.isafe.org

staysafe.org: Online Safety & Security Is All About You
www.getnetsafe.org

Center for Safe and Responsible Internet Use
www.cyberbully.org

WiredSafety.org—the world's largest Internet safety and help group
www.wiredsafety.org

National Center for Missing & Exploited Children: CyberTipline
www.cybertipline.com

TeenAngels: A Division of WiredSafety.org
www.teenangels.org

SafeTeens
www.safeteens.com

Help Net Security
www.net-security.org

Spyware Warrior
www.spywarewarrior.com

StaySafeOnline.org: National Cyber Security Alliance
www.staysafeonline.info

Additional Resources from www.films.com • 1-800-257-5126

Cyberbullying: Cruel Intentions

- **DVD/ VHS**
- **Preview clip online**
- **Close captioned**
- **Correlates to educational standards**
- **Item # 36546**

The teenage years have always been tough—but digital technology has raised the dangers of the social battlefield to a whole new level. This ABC News program reports on how cell phones, digital cameras, and personal websites encourage and amplify the frequent cruelty of teen behavior. With the help of an experiment conducted by Brigham Young University child development researchers, the program analyzes the behavior of a group of teenage girls as they use online verbal innuendos and emotional attacks to vie for attention and create a social hierarchy. The program also looks at the difficulties parents face in monitoring what kids do on the Internet. (40 minutes) © 2006

Cyberbullies

- **DVD/ VHS**
- **Preview clip online**
- **Close captioned**
- **Correlates to educational standards**
- **Includes viewable/printable instructor's guide**

"Students will be familiar with the many types of cyberbullying discussed."—*School Library Journal*

- **Item # 34758**

Chat rooms, blogs, and instant messaging have become standard forms of communication for many young people. Unfortunately, they have also become popular ways to harass others. This program is designed to prevent children and teenagers from falling victim to cyberbullying, using dramatizations and Q & A discussions to expand awareness of the issue. The video discusses cyberbullying warning signs, common patterns of abuse, and questionable online activities and destinations to stay away from. It also presents strategies for responding when cyberbullying occurs, and outlines legal problems involving privacy and libel that young Internet users should be aware of. (19 minutes) © 2006

Sc@mmed: Online Identity Theft

- **DVD/ VHS**
- **Close captioned**
- **Item # 37475**

Bouncing between Canada and the U.S., *Sc@mmed* exposes an urgent problem of global proportions: phishing, the illegal gathering of others' personal information online in order to steal all their money—and even their identities. Through the cautionary stories of two people who got burned, this program shows how cybercriminals use scam spam and spoof Web sites to trick people into willingly giving up their most sensitive financial and personal information. Crooks go phishing all around the world every day; help your students avoid becoming their next victims. (25 minutes) ©2005

Information Literacy: The Perils of Online Research

- **DVD/ VHS**
- **Preview clip online**
- **Close captioned**
- **Correlates to educational standards**
- **Includes viewable/printable instructor's guide**
- **Recommended by *The Social Studies Educator* and *Educational Media Reviews Online.***
- **Item # 35675**

In a world of information overload, information literacy has become a survival skill. But what exactly does information literacy mean? With a focus on the Internet, this video explains how to conduct solid online research by collecting information in an organized, efficient, and ethical way. Professor Maurita Holland of the University of Michigan School of Information provides expert commentary and guidance on a range of research activities, including evaluating the credibility of Web content, documenting online sources, and paraphrasing—not copying—the words of others. Additionally, a high school teacher and a graduate student demonstrate real-world examples to reinforce the challenges and rewards of online research. The consequences of plagiarism and shaky facts are emphasized. A viewable/printable instructor's guide is available online. Correlates to all applicable state and national standards. A Cambridge Educational Production. (21 minutes) © 2006

The Big Poker Gamble

- **DVD/ VHS**
- **Preview clip online**
- **Close captioned**
- **Item # 36231**

By day, Jane is an unassuming single mother. At night she's a high-stakes poker player—thanks to the Internet. So far Jane has won thousands of dollars, as have many online gamblers, while others have lost huge sums. This program looks at the explosive cyber-gambling industry, examining some leading sites and profiling men and women whose lifestyles now revolve around card-playing by computer. Doug's story conveys the hard, all-too frequent reality of sustained losing, shedding light on its social and personal consequences. Additional interviews with gaming promoters, tournament champions, and government regulators round out this eye-opening investigation. (28 minutes) © 2005

Teens Hooked on Porn

- **DVD/ VHS**
- **Preview clip online**
- **Close captioned**
- **Item # 37386**

Whether they live in America, Britain, or elsewhere, most teenage boys have been exposed to some form of pornography. But the Internet has radically escalated that exposure—to the point at which many adolescents are addicted. This program follows the stories of teenage porn addicts as they struggle with the issues that drive their behavior—although not all are open to soul-searching. Darryl, age 17, doesn't think he has a problem, but 16-year-old Malcolm has recognized his addiction and has begun seeing a therapist. Colin, age 14 and a devout Christian, needs help too but is unsure about approaching his pastor. All of their stories are tied together by issues of anger, aggression, and inhibition, and raise questions about the role of parents. A BBCW Production. (57 minutes) © 2007

Spam

- **DVD/ VHS**
- **Preview clip online**
- **Close captioned**
- **Correlates to educational standards**
- **Includes viewable/printable instructor's guide**
- **Item # 34208**

What is spam? How do spammers get their unwanted offers into your in-box? And how can the flow of electronic junk mail be stopped? Filmed in news report style, this program explains how shady advertisers send spam and then presents proactive strategies for combating it: spam filters, blacklists and white lists, opt-in and opt-out protocols, anti-spam legislation with real teeth, and greater cooperation between legitimate businesses, Internet and online service providers, and consumers. Spammer techniques—how spammers harvest e-mail addresses, use open relays and spoofing to cover their tracks, and more—are revealed. (30 minutes) © 2004

Computer Worms and Viruses

- **DVD/ VHS**
- **Preview clip online**
- **Close captioned**
- **Correlates to educational standards**
- **Item # 33538**

Computer bugs are no mere prank. A disruption of global communications networks by today's sophisticated worms and viruses is costing companies billions and can do lasting damage to the world's economic health. This NewsHour program begins by defining these binary invaders and then examines the escalating security challenges of keeping networks free of infection. Members of the Computer Emergency Response Team at Carnegie Mellon University and other white hats discuss proactive ways to detect and then block electronic intruders through single-user protocols and enterprise-wide defenses. (10 minutes) © 2003