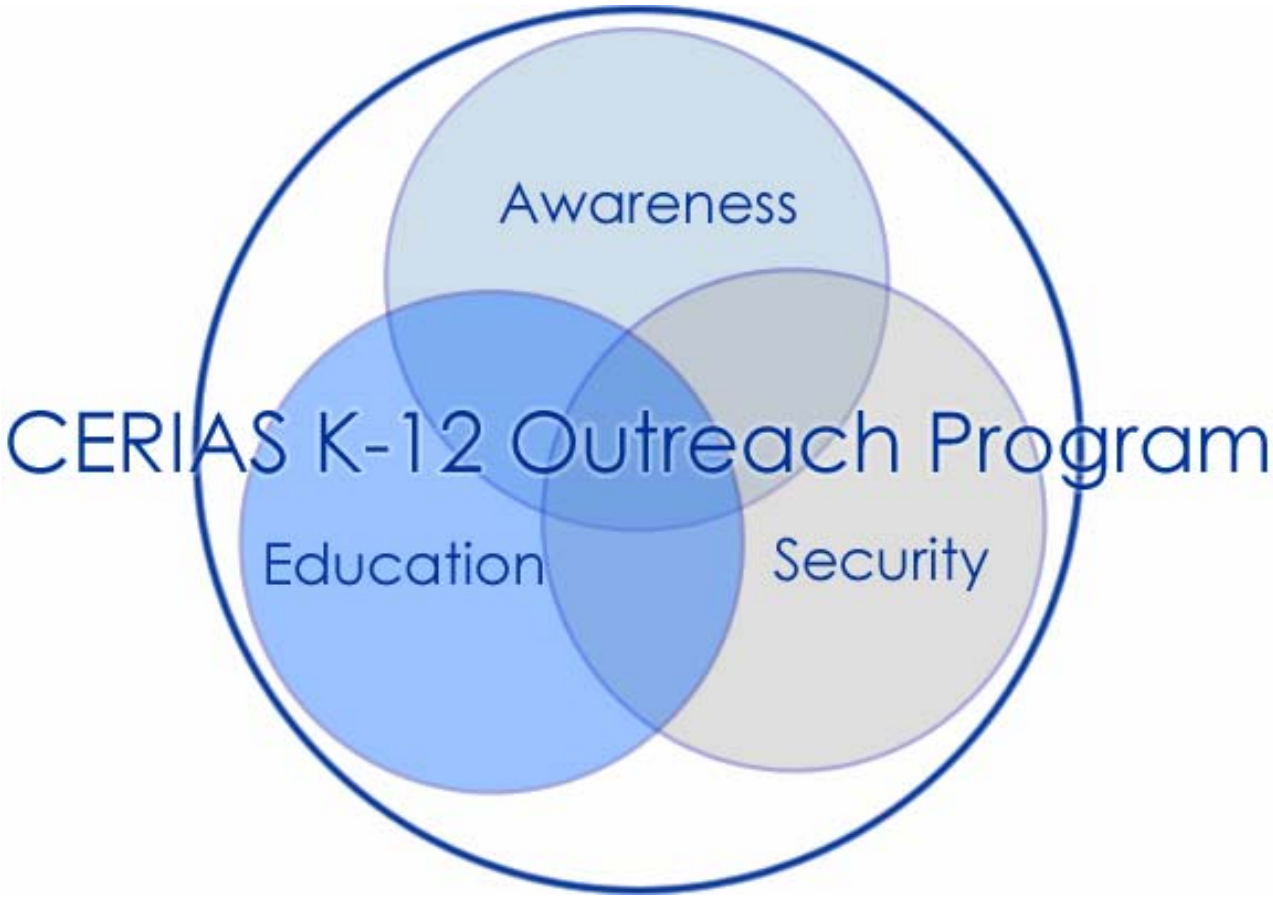


PURDUE
UNIVERSITY

The Center for Education and Research in Information Assurance and Security

Purdue University ● 656 Oval Drive ● West Lafayette, IN ● 47907-2086
(765) 494-7871 ● Fax (765) 496-3181 ● k-12@cerias.purdue.edu ● www.cerias.purdue.edu

The CERIAS K-12 Outreach Program mission is three fold: to increase the security of K-12 information systems, integrate information security as a discipline into the K-12 curriculum, and to raise parent and community awareness of information security issues through K-12 schools. Building upon existing work, the program will continue to grow and fulfill its mission through collaboration with K-12 schools in the state of Indiana, outreach entities on the Purdue University campus and nationwide, Indiana Service Centers, and CERIAS sponsors.

This document highlights current outreach efforts and initiatives. If you are interested in pilot testing new or using existing materials, partnering, or if you would like to learn more about the CERIAS K-12 Outreach Program, please visit our website at

www.cerias.purdue.edu/k-12/

or email us at

k-12outreach@cerias.purdue.edu

Purdue University ● 656 Oval Drive ● West Lafayette, IN ● 47907-2086
(765) 494-7871 ● Fax (765) 496-3181 ● k-12@cerias.purdue.edu ● www.cerias.purdue.edu

Table of Contents

Goal 1: Community Awareness through K-12 Schools

While there is a significant need across public and private sectors for educating and distributing information to the users and administrators of information systems, home users are particularly isolated from awareness and training opportunities in information security. It is our mission at CERIAS to enhance the public's understanding and acceptance of information protection through awareness, training, and education; partnerships with K-12 schools leverage existing connections to local community life and help to bring a seemingly remote and ignored topic from the classroom to the kitchen table. The two initiatives described below highlight work being done in this area.

A. Information Security Newsletter Series

The information security newsletter series is a collection of short, informative articles intended to be included with school newsletters. Written in an easy-to-understand, conversational tone, the information security newsletter series is an effective way to inform parents about the basics of information security.

B. PTA Presentation: Teaching Your Children to Use the Internet Safely and Responsibly

Internet usage continues to escalate, particularly among children. While this powerful tool offers many possibilities for growth and learning, it also presents many security threats to children and to their families.

This presentation familiarizes parents with information security issues and introduces the idea of creating a contract with their children to help manage their family's use of the Internet. This contract can help protect families against Internet dangers by helping parents communicate with their children about cyber-ethics, cyber-safety, and cyber-security issues. Creation of the contract can also reduce family conflict concerning Internet use by setting clear guidelines for use and establishing consequences for lack of observance of guidelines. Utilizing the defenses of prevention and collaboration, the Internet Use Contract can enable families to use the Internet safely and responsibly.

Delivered by CERIAS personnel experienced in information security issues and K-12 education, this presentation can be modified to fit any specified time frame from 30 minutes to 2 hours. In addition, this presentation is also available in the form of a self-instructional document.

Purdue University ● 656 Oval Drive ● West Lafayette, IN ● 47907-2086
(765) 494-7871 ● Fax (765) 496-3181 ● k-12@cerias.purdue.edu ● www.cerias.purdue.edu

Goal 2: Integration of Information Security into K-12 Standards and Curriculum

There is an alarming shortage of information security and information technology professionals in the state of Indiana and nationwide. At CERIAS, we believe that the solution to this problem begins early. Integrating information security topics into the K-12 curriculum and aligning it with state and national standards will help alleviate the shortage by increasing the skills of the entire future workforce. Integrating security topics into the curriculum will also help address issues of online safety, critical literacy, and transfer of ethical behavior to the online environment. Integrating information security topics into the curriculum promotes cross-curricular studies and real-world problem-solving.

A. K-5 Information Security Lesson Plans

We have developed a series of lesson plans to help teachers integrate information security concepts into their classrooms. Because we know that time is a critical resource for teachers, we have developed these lessons to be very easy to use. Aligned with Indiana academic standards, our lessons are complete with material lists, entry competencies, objectives, and step-by-step teaching instructions. Many of these materials can be easily modified to fit both younger and older audiences.

These lessons are cross-curricular and can be used to demonstrate the real-world applications of the various disciplines.

HOW TEACHERS CAN GET INVOLVED: We need you to share your expertise with us by trying out any of the lessons in your classroom and providing feedback. We are looking to continually improve the lessons so that we can best serve your students.
We are available to help facilitate the lessons with your students or to work with groups of teachers on strategies for implementing the lessons yourselves.

B. Middle School Information Security Materials

Two surveys concerned with information security literacy were given to almost 500 middle and 9th grade students in three schools in Indiana—two rural middle schools and one urban high school. The results of this survey led to the creation of lessons and activities geared toward the needs of middle school students. The lesson plans and materials, "Your Guide to Safe Surfing: Learning about the Internet" is aligned with state and national science, math, history, technology, and language arts standards.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

Goal 3: Increase the Security of K-12 Information Systems

The security of cyberspace rests on the security of all its components. Even K-12 institutions contribute to or detract from our nation's cyber security. Unfortunately, few school systems have the in-house expertise or funding to mitigate risks to the security of their information systems. To ensure the security of a school's information, the availability of services critical to learning, and the safety of a school's constituents, CERIAS aims to take a multi-level approach to solving the information security dilemma.

A. CERIAS Workshops for the K-12 Technology Coordinator

Specifically geared toward K-12 technology coordinators, this series of workshops is designed to help ensure that the security risks to schools are known by all stakeholders and that they are made aware of the latest protection solutions to those risks. Workshops are conducted at the Wabash Valley Education Center (WVEC), with the intent to eventually replicate the workshops in other Indiana service centers in order to reach the entire K-12 community. Topics include:

1. Introduction to Information Security
2. Risk Analysis
3. Legal Issues and Regulations
4. Creating & Auditing School Security Practices
5. Building an Awareness and Training Program
6. Intrusion Detection: An Overview

B. School Vulnerability Assessments

InfoTex, an information technology consultancy and a sponsor of CERIAS, has provided five pro bono vulnerability assessments to a group of participating schools. The results of these assessments will serve several purposes:

1. Increase the security of participating schools' information systems by providing a detailed report of existing vulnerabilities as well as future suggestions for network design and configuration.
2. Provide accurate, anonymized, scalable data on the state of information security in K-12 schools that can be used to support future educational initiatives.

C. Purdue University/Indiana K-12 Schools Joint Project

CERIAS is partnering with the Purdue University Schools of Technology and Education, the WVEC, and select K-12 schools to write a grant proposal to fund continued and expanded work in this area. The grant would establish a service-learning course wherein graduate students will teach technology coordinators more about information security in a one-on-one manner. The graduate students will receive course credit and the schools' technology coordinators will get ongoing, sustainable training on new security threats, vulnerabilities, and countermeasures.

Purdue University ● 656 Oval Drive ● West Lafayette, IN ● 47907-2086
(765) 494-7871 ● Fax (765) 496-3181 ● k-12@cerias.purdue.edu ● www.cerias.purdue.edu

D. Keeping Information Safe: Practices in K-12 Schools

This project, funded by the Indiana Higher Education Telecommunications System (IHETS), serves several populations: 1) in-service K-12 educators who hold a bachelor's degree or higher in education or a related field, 2) K-12 support staff who operate computers as end-users and/or handle sensitive and confidential information, and 3) Purdue University undergraduates enrolled in educational technology courses. The output of this project will be a set of self-instructional multimedia modules focusing on best-practices in end-user information security.

Purdue University ● 656 Oval Drive ● West Lafayette, IN ● 47907-2086
(765) 494-7871 ● Fax (765) 496-3181 ● k-12@cerias.purdue.edu ● www.cerias.purdue.edu

People

Dr. Melissa Dark

Dr. Melissa Dark teaches information security courses in the Technology Management Masters of Science degree program and has guest lectured to a variety of audiences including college faculty, trustees, executives, and end users, on information security issues. Dr. Dark works with a variety of organizations such as the Indiana CPA Society, the Indiana State Police, the Indiana FBI, the US Secret Service, and InfraGard to broker security education. Dr. Dark is currently involved in a nation wide curriculum initiative to determine core information security topics to be included in accredited information security programs at the undergraduate and graduate levels. Her research interests include methods for effectively transferring new knowledge into educational systems and organizations, and the return on investment for doing so.

Matt Rose

As an instructional designer at CERIAS, Matt Rose designs and develops educational products and solutions in information assurance and security in a variety of formats and for a wide range of audiences, including corporate management, IT professionals, home users, end users, and the K-12 educator. Matt 's other responsibilities include identifying and assembling offerings for short courses and workshops, in which capacity he serves as both a coordinator and instructor, and project manager of special projects and initiatives. An assistant professor in the School of Technology at Purdue, Matt also teaches TECH 623(W): Information Security; before working at CERIAS, Matt taught AP Language and Composition at an Indiana high school. Matt is a member of the Association for Computing Machinery (ACM), the Federal Information System Security Educator's Association (FISSEA), the International Society for Performance Improvement (ISPI), InfraGard, and the ISTE.

Matt Jonkman

Matthew Jonkman has been involved in IT since the mid-1980s. He has a strong background in banking and network security, and network engineering. Matt's certifications include CISSP, Comptia A+, CCSE (Checkpoint Certified Systems Engineer), and CCSA (Checkpoint Certified Systems Administrator). Matt spent 5 years serving in the Army before attending Indiana State University and the Rose-Hulman Institute. After college he worked for Sprint's Internal and Managed Security division, as well as for a major Midwestern bank and financial services corporation. Matt is currently the Senior Security Engineer for InfoTex, an Indiana-based security and consulting firm offering a full range of general and security specific consulting services and Security Audits, as well as Managed Intrusion Detection and Managed Firewall Services.

Dr. Jennifer Richardson

An Assistant Professor of Educational Technology in the School of Education, Professor Richardson's research focuses on K-12 technology integration including practices, professional development, diffusion of technology integration plans, and impediments to successful implementation. She is also involved in research of online learning environments and how social presence and interactions affect students' perceptions, satisfaction, and learning.

Purdue University ● 656 Oval Drive ● West Lafayette, IN ● 47907-2086
(765) 494-7871 ● Fax (765) 496-3181 ● k-12@cerias.purdue.edu ● www.cerias.purdue.edu

APPENDIX A:
RELATED MATERIAL FOR GOAL 1

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

Information Security Newsletter Series: List of Subjects

1. Information Security for the Home—An Introduction
2. Risks to Information Security
3. Information Security Threats and Vulnerabilities
4. The Home IT Specialist
5. Passwords: Your 1st Line of Defense
6. Broadband vs. Dialup
7. Cyber Ethics
8. Cyber Crimes and Your Children
9. Safe Online Shopping
10. Email Attachments
11. Spam Email
12. Computer Virus Identification and Prevention
13. Computer Backups
14. Firewalls
15. Identity Theft
16. PTA Presentation
17. Information Security Week In-School Announcements

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

Information Security Newsletter Series: Information Security for the Home – An Introduction

Information security is a term used to describe the process of protecting information and services from misuse or destruction. When we use the term in the context of the home, we use it to describe the steps we take to make sure that our computers, the information we have stored on it, and the people who use it are kept safe from harm. Unfortunately, information security in the home is often overlooked. But by taking a few moments to learn a few key concepts and concerns, you can make sure that you are keeping your family and your information safe.

Goals of Information Security

Let's start by investigating the purpose of information security. We want to achieve three main goals by practicing good information security. Other goals, such as the safety of your children and the privacy of your personal information, depend upon these goals:

- **Confidentiality**: Information is available only to those who rightfully have access to it.
- **Integrity**: Information should be modified only by those who are authorized to do so.
- **Availability**: Information should be accessible to those who need it when they need it.

Information Security Strategies

Most homeowners take steps to protect their homes by installing locks on their doors, smoke detectors in the hallway, or even a security system. Obviously, we do these things for several reasons, but primarily to keep our families and our possessions safe. It is the same with information security. An unsecured computer is an invitation to browse through your and your family's life. To keep this from happening and to achieve the above goals, we use three strategies:

- **Prevention**: This strategy represents the need to install the proper software and/or hardware and take the proper precautions in order to stop an attack before it occurs.
- **Detection**: This strategy represents the need to keep your system up to date on the latest types of attacks in order to understand when your PC has been damage or is at a high risk.
- **Recovery**: This strategy represents the need to form a plan of action in order to reverse, if possible, damage done to your computer and/or personal information after an attack has occurred.

This following collection of newsletters will help to educate you on the possible risks of not keeping up-to-date on information security measures, how different attacks can affect you, and how to prevent damage to your computer and/or personal information. Focusing on the above goals and strategies while reading this collection of newsletters will not only help you to better understand the specifics of information security, but it will also help you to learn how to better implement these practices into your home.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

Information Security Newsletter Series: Risks to Information Security

Computer Hackers and Your Computer's Security

In our first article on information security, we learned that information security involves the prevention and detection of unauthorized use of a computer or information system. We also learned about the three main goals of information security: confidentiality, integrity, and availability. Today, we will investigate risks to information security and ways to prevent these risks.

If you're like many people, you're probably wondering who, exactly, would really want to break into your computer, and why. After all, your home computer is much less enticing than, say, a bank's computer, right? This may be partially true, but unfortunately, hackers don't care about who you are. They want to gain access to your computer to use it to attack other computers or take your personal information to use against you or use to steal your identity.

Here's how a typical hacker operates: A hacker scans the Internet for an "open" computer, a computer with little to no protection on it (we refer to this as the "lowest hanging fruit"). He then breaks into the computer, and then uses it to attack other computers. Why? This way he can keep his whereabouts a secret. Sometimes a hacker actually breaks into several computers, and uses them all to attack one computer at the same time.

Even if your computer is connected to the Internet for only a short time, your computer may still be a target. Being online for even a short time gives intruders the chance to take enough information to steal your identity or cause damage to your or someone else's computer.

How easy is it for a hacker to break into your computer? Unfortunately, intruders are discovering new ways to gain access to your information every day. When holes in the system are discovered, however, computer vendors will often develop patches to address the problem. Even though they do this, it is up to you to obtain and install the patches, or correctly configure the software to operate more securely. Most incidents can be prevented if users would keep their computers up to date with patches and security fixes. Some software even has default settings that allow others to access your computer unless you change the settings, such as chat programs or web browsers.

The only way to make any information system more secure is to learn about the ways to make it so. Although this article only touches the surface of even the basic risks to information security, you will learn more about making your time online and your own information system safer and more secure in the articles that follow. Although no system is ever impossible to break into or free of risk, learning the ways to make your own information system more secure will help reduce the chances of anything harmful happening to your information.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

Information Security Newsletter Series: Information Security Threats and Vulnerabilities

Threats to computers and information systems are quite real. In previous newsletters, we've discussed hacking risks to your information systems, but this is just as mall element of the big picture of threats and vulnerabilities to information security. Identifying threats are only part of the picture; once threats are identified, it is up to you to find the vulnerabilities in your information system and find ways to keep these threats from occurring.

Although threats to information systems are evolving and abundant, they can all be broken down into three categories:

Natural Threats: These can best be thought of as threats caused by Mother Nature—floods, quakes, tornadoes, temperature extremes, hurricanes, and storms are all examples.
Intentional Threats: Computer crimes are the best examples of intentional threats, or when someone purposely damages property or information. Computer crimes include espionage, identity theft, child pornography, and credit card crime.
Unintentional Threats: These threats basically include the unauthorized or accidental modification of software. Have you ever accidentally deleted an important file, or tripped over a power cord?

Finding the Vulnerable Spots
Now we need to be able to determine how your information system is vulnerable to the above threats. The two main vulnerabilities to home users are to your operating system (OS) and to your Internet connection.

An OS is the program that essentially "runs" your computer. Although Microsoft Windows and Apple Mac O/S are the most well known operating systems, others that you may have heard of include Linux and UNIX. If someone knows what OS you're running on your computer, the more likely he'll be able to access your system and exploit weaknesses within it. Making sure that you frequently check for security patches and updates will help keep your system more secure.

Internet connections are also susceptible to threats. Broadband connections are more susceptible than dialups because these services are always connected to the Internet, making it easier for people to find you and take your information or send you a virus. Purchasing a firewall and an anti-virus program will help keep your information safe from attack when connected to the Internet for long periods of time.

Being aware of threats and vulnerabilities is the first step in making your information system more safe and secure. Although no system is truly safe from all threats, knowing ahead of time just what could compromise your information and becoming educated in ways of preventing these threats will make you more prepared for any attack and give you the chance to protect yourself from it.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

Information Security Newsletter Series: The Home IT Specialist

Just as if your home were a business, you are the Information Technology (IT) Specialist of your home computer. As that IT Specialist, it is your responsibility to protect your computer—and any data stored in it. *You are in charge of the security of your home system*, meaning you have the responsibility of identifying any unusual activity on your system and responding to that activity in an effective and timely manner. This could entail fixing security weaknesses in your Internet service through the use of firewalls and virus detection software, repairing operating system difficulties through patches and updates, and simply staying abreast of these problems in general.

Earlier, we discussed the four major security threats: environmental natural, environmental manmade, human intentional and human unintentional, as well as the two major vulnerabilities associated with computers, which are through Internet connections and operating systems.

In order to effectively prevent vulnerabilities and threats from occurring, it is up to you as the IT Specialist to create countermeasures for them. Although no system can be 100% secure, having countermeasures in place can certainly lessen the likelihood of risks or vulnerabilities from being exploited on your computer.

There are three common countermeasures that you can easily implement on your home computer:

Technical: Technical countermeasures mean using software to protect your system, including installing firewalls and anti-virus software, as well as taking steps like changing the security settings of your Web browser.

Procedural: Procedural countermeasures are activities that you establish in order to prevent the exploitation of your computer. This includes scheduling scans and updates for an anti-virus program, password protecting accounts and screen savers, and backing up important data on disks.

Contracts: A set of easily-accessible, written and signed contracts will ensure that your children are following the rules you have set out for them in regards to using the computer and the Internet.

Summary

Remember that, although no system can ever be 100% tamper proof, having some simple countermeasures in place will help keep many intruders at bay and your computer safe. As your home's IT Specialist, it's up to you to make sure that these countermeasures are used and followed. It's also important to have consequences for not following policies and procedures. Grounding a child from using the computer for a week for not running the anti-virus software on a downloaded attachment might make him think twice before not doing it again.

Purdue University ● 656 Oval Drive ● West Lafayette, IN ● 47907-2086
(765) 494-7871 ● Fax (765) 496-3181 ● k-12@cerias.purdue.edu ● www.cerias.purdue.edu

Information Security Newsletter Series: Passwords: Your 1st Line of Defense

Protecting your computer with a password is a common method of ensuring that only those with permission can access it. However, passwords are effective only as long as you use ones that are easy to remember and difficult to "break," and that are changed on a regular basis. Did you know that anyone with a little bit of technical know-how can download a program off the Internet and use it to break weak passwords? These programs use "brute force" and "dictionary attacks" to try every possible combination of words and letters to break into your account. The best way to combat this very real threat is to write strong passwords. The following simple rules for writing and using strong passwords will keep your computer more secure, decreasing the chance of compromise.

Your Password: Strong or Weak?

Strong Passwords:

- Are 8 or more characters long
- Contain combination of upper and lowercase letters, numbers, and symbols ($ch00LrU135 = school rules)
- Are passphrases: Choose a line or two from a song or poem and use the first letter of each word. For example, "It is the East, and Juliet is the Sun" becomes "IstE,@J1tS"
- Are changed on a regular basis
- Are easy to remember and are not written down
- Are not used over and over again for different programs and websites
- Are typed quickly, making it harder for someone to steal by eavesdropping

Weak Passwords:

- Contain your login, your name, your maiden name, your spouse's name, your children's names or your pets' names in any form as your password
- Contain publicly accessible information about yourself, such as social security number, license numbers, phone numbers, address, birthdays, etc.
- Contain a word found in a dictionary of any language
- Are made of all numbers or all the same letter
- Are saved in the "Remember Password" function on mail or website browsers
- Are written down
- Are shared with others

Summary

Passwords make it as difficult as possible for someone else to access your information. If you follow the strong password practices outlined above by writing strong passwords or passphrases, changing them frequently (every 3-6 months), and keeping them safe from others by not sharing them or writing them down, you will be able to keep your computer and your personal information—such as your banking and credit card information—safe.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

Information Security Newsletter Series: Broadband vs. Dialup

Parents across the nation have already been introduced to broadband Internet connections such as cable or DSL (Digital Subscriber Lines) by their children, who want to have a faster, higher-quality connection. Whatever your reason for considering purchasing a broadband connection, it is very useful—and important—to know the differences between broadband and dialup Internet connections and the advantages and disadvantages between each of them before making a decision to go high-speed.

The fundamental difference between dialup and broadband Internet connections is the manner in which the connection is made from your PC to the Internet. A dialup service connects to the Internet through your phone line. The modem in your PC "calls" an Internet Service Provider (ISP) and connects with a maximum speed of 56,000 bytes per second, better known as a 56K speed connection. Each time your PC dials into the ISP, it is assigned an Internet Protocol (IP) address, which you can think of as an "Internet address." A different, unique IP address is assigned at the beginning of each visit so that the ISP can recognize your PC and make sure you can send and receive email, surf the Internet, and so on; basically, this address lets your ISP know where to send the information you are requesting through your modem. In terms of hackers, in order for someone to gain access to your computer, it would be necessary for them to know your IP to successfully do so. The fact that your IP address constantly changes essentially makes your Internet connection more secure.
needs to send data to another computer, it has to know its IP address.

In contrast, when you connect to the Internet via a broadband Internet connection, the process is slightly different. Once your PC is connected to the ISP through a cable or DSL connection, it *remains connected* until the cable box or DSL line is disconnected or physically unplugged. A DSL connection runs through unused wires in your existing phone line without disruption and can translate data at 5 million bytes per second, or 5Mbps. Broadband services are often referred to as "always on" services because it is not necessary to make a setup call to your ISP each time you wish to access the Internet; this means that once you are assigned an IP address, you keep it until you request it to be changed. We'll learn how to do this in a later newsletter.

Connection speed and price are two important considerations when choosing between dialup and broadband. Dialup connection speeds make it more difficult to view certain types of media, such as video, and it can take much longer to download and open email attachments, play online games, and so on. Although the slower connection speed is a disadvantage for dialup users, there are also a few advantages to using this type of connection, which include lower monthly charges and a higher level of security. The cost difference is obvious when comparing the $20-30 per month subscription fee for dialup and the $50-60 per month subscription fee for most broadband services. In terms of security, because the connection is not "always on" and because you are assigned a different IP address each time, it is slightly more difficult to be attacked over the Internet, although nothing is ever fool proof and risks still do exist. The advantages of a broadband connection can sometimes outweigh some of the disadvantages. The increased connection speed allows for ease in initial connection, duration of connection, no additional phone charges that may apply in dialing into an ISP, and variability of Internet use, such as an increase in allowable file viewing size. However, if you do choose a broadband connection, you'll need to purchase a firewall—which we'll learn more about later—to keep your computer "invisible" to the outside world.

In the ongoing debate of which is better dialup or broadband, there isn't really a clearly correct answer. This question can only be answered by looking at your needs and resources and comparing them to what each option has to offer. If you use the Internet to check email, stock quotes, and visit the occasional website, dialup will be sufficient. But if you frequently download large media files, play games over the Internet, and view sites that are high in image content then you may be more satisfied with broadband service.

Purdue University ● 656 Oval Drive ● West Lafayette, IN ● 47907-2086
(765) 494-7871 ● Fax (765) 496-3181 ● k-12@cerias.purdue.edu ● www.cerias.purdue.edu

Information Security Newsletter Series: Cyber Ethics

Is there a difference between ethics in the real world and ethics online? While the answer to this question might seem obvious to parents, for many children, there is a very real—and potentially dangerous—disconnect between ethics in the real world and cyberspace. A recent poll found that nearly half of the elementary and middle school students who responded said they don't believe hacking is a crime. Why is there this divide between real-world and cyber ethics, and what can parents do to make sure that their children practice ethical behavior when online?

The Ethical Divide

Is the Internet that much different than the real world? After all, a crime *is* a crime. There are two characteristics of the Internet that make it difficult for children to transfer ethical behavior to the online environment:

The first characteristic is the feeling of anonymity. The *New Yorker* once published a cartoon with the punch line, "On the Internet, nobody knows you're a dog"; the cartoon was making the point that it is easy to feel invisible on the Internet. Children often believe that they are "invisible" online because they cannot be identified and can get away with more (this actually isn't true—modern computer forensics makes it very easy to track a user online). Many young children also feel that regular rules don't apply to the Internet.

The second characteristic is distance. On the Internet, many people do and say things to others that they would never consider doing to someone face-to-face. Because children cannot see the direct consequences of their actions, they often think that what they are doing won't harm anyone else. Of course, parents know that this is not true. Actions on the Internet still have the same repercussions as actions in the real world.

Promoting Ethical Behavior Online

Now that we know a little bit about why children don't transfer ethical behavior to the online environment, we can examine a few strategies for promoting ethical behavior:

- **Communication**: The most obvious strategy involves taking the time to talk with our children about acceptable and unacceptable online behavior. Children need to understand that their actions can impact others, and that they should practice the same etiquette online as they would in the real world. Make comparisons between online and real-world ethics and point out that they are, in reality, the same.
- **Modeling**: When online, model ethical behavior and point out areas where ethical behavior makes a difference.
- **Contracts**: Sign a "contract" with your children that outlines the type of behavior you expect, as well as the consequences for breaching the contract. What should be in this contract? A good source of information to draw from is the Computer Ethics Institute's "10 Commandments of Computer Ethics," which you can find online at <www.brook.edu/dybdocroot/its/cei/default.htm>.

Summary

Children need to know that using the Internet is a privilege, not a right, and that improper use has consequences. Sitting down with your child and discussing these issues is the best way to make sure he does not use the Internet in a harmful or malicious way.

Information Security Newsletter Series: Cyber Crimes and Your Children

ISPs, parents, software companies, and schools have been doing their best to protect children from risks online, but there is still a need to protect the Internet from children who may wish to find ways to abuse and exploit it. To prevent children from participating in these cyber crimes, it is important to define cyber crime and examine the losses from cyber crime, as well as the ways to keep your children from becoming perpetrators in these crimes.

The US Department of Justice categorizes cyber crime in three ways:

The Computer as a Target (using a computer to attack other computers): Did you know that the majority of cybercrimes in this category are committed by children? As recently as September, 2003, a teenager was arrested for creating a devastating computer virus. How did he learn to do this? A simple Internet search will reveal all the tools necessary to create viruses and hack into others' computers. Hacking can take a variety of forms, ranging from stealing passwords and classified information to vandalizing Web sites. Unauthorized entry into an information system through hacking or viruses has serious legal consequences. Talk with your child about the ethical and legal implications of hacking.

The computer as a weapon (using a computer to commit real world crimes) Take, for instance, email. Children believe email is harmless because they don't see the impact on the person who receives it. A growing trend with the use of email and chat programs is harassment; children are saying things to other children—both at school and in other communities—that they would never say face-to face. Parents need to teach their children about appropriate communication through email and chat programs.

The computer as an accessory (using a computer to store illegal files or information): The Internet is a useful tool for finding information in a quick and convenient way. Even though much of this information is available for everyone to use, many products and services found online are not permissible to be reproduced or downloaded, especially music and purchasable programs. Popular peer-to-peer software programs make is easy to share copyrighted material and actually encourage downloading, but it is a violation of copyright law to take music or software from the Internet without the permission of the owner. It is easy for children understand why the theft in the real world is wrong, but it is difficult for them to understand theft of intellectual property. Teach your children not to download pirated or counterfeit material.

Summary

Although it may not seem real, cyber crime has actual victims and very concrete consequences. Whether it's loss of money, time, pride, or life, someone or something is always a victim. The best way to prevent cyber crime is to educate children about the types of cyber crimes, the cost of cyber crime to the victims, and the consequences for committing such crimes.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

Information Security Newsletter Series: Safe Online Shopping

Online shopping may be one of the most useful services that the Internet age has brought us; online shopping is convenient and often presents us with more choices and better deals than we can find locally. There are, of course, a few potential dangers to online shopping, including fraud, identity theft, and privacy invasion. Fortunately, by staying informed and being aware of a few key factors, you can ensure that your online shopping experience is safe and successful.

So what should you watch out for when shopping online? The following key items are important to consider:

The Seller: Just as in the physical world, you should always ask yourself if you trust the seller before you buy anything from them. Use your gut instincts when purchasing online; if a website looks unprofessional—if it doesn't contain any contact information, looks shoddy, or contains typographical errors—you probably don't want to purchase from it. Judging a seller is more difficult in online auctions. In this case, look to see if the seller has any reviews by other customers. If the deal seems too good to be true, it probably is; modern con artists create fake websites and send out phony emails to lure unsuspecting shoppers into giving away their hard-earned money.

The Product & Terms: Again, if a deal seems too good to be true, it probably is. Make sure that you are going to get what you think you're buying. Also, while it is convenient to shop online, it is not always as convenient to return an item or resolve a dispute. Make sure you know the shipping policy, check the return policy, and before you confirm your purchase online, double check the price and quantity.

Security: Credit card transactions are a mainstay of online shopping. To ensure that your credit card and personal information stays out of the wrong hands, check to see that the website uses SSL encryption. Before entering *any* personal information on a web site, check to see that the web address begins with *https://* instead of *http://*. If you are uncomfortable giving out financial and personal information online, many reputable sites also have a phone in option. Browse the seller's online catalog, then order via phone.

Privacy: Online shopping means that the seller will be collecting your personal information. Make sure you know *how* the seller intends to use your information before you give it to them. Reputable sites will post an easy to understand privacy policy on their site. A good privacy policy should tell you what information is collected (note that a website should never ask for your social security number), how it will be used, and whether or not you can "opt out." Make sure you agree to a site's terms before you order; otherwise, you may find yourself flooded with spam and telemarketing calls.

Email Confirmations: Related to both privacy and security are the email confirmations that many sellers send after you have made a purchase. Often these emails will contain confidential information, such as your name, address, telephone number, and credit card information. Email communications are not considered secure; if this information falls into the wrong hands, you could become the victim of identity theft. So when given the option, choose not to receive email confirmations.

Online shopping is a liberating experience, but like many things on the Internet, it is not without its potential pitfalls. Take the time to evaluate the security and privacy of the website, the product and shipping information, the return policy, and the seller's reputation before you buy, and you will have a safe and successful online shopping experience. If you would like to learn more about safe online shopping, visit www.safeshopping.org for more tips or www.ftc.gov/bcp/menu-internet.htm for information about online shopping hoaxes and scams.
Shopping online eliminates that factor. By remembering this fact and following these few simple suggestions, online shopping experiences should be safe and painless.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

Information Security Newsletter Series: Email Attachments

Even if you consider yourself to be a knowledgeable user of the Internet and email programs like Microsoft Outlook, Outlook Express, Eudora, or Netscape, you might not always be aware of the ways that email can be used to affect your computer and how to prevent email attacks. Let's take a look at a few different attacks and the countermeasures that will keep you safe:

Viruses: Viruses and other types of malicious code are often spread as attachments to email messages. Before opening attachments, be sure you know where the attachment came from and what type of file it is. Many email viruses are known to exploit hidden file extensions. The files attached to these messages may appear to be harmless text, MPEG, AVI or other file types, but the file is actually malicious script or executable virus programs—.vbs, .exe, or .bat files, for example. Always read the entire file name before opening attachments.

Viruses and malicious code might be distributed in amusing or enticing programs, particularly around the holidays. It's always best to never run a program unless you know it to be made by a person or company that you trust. Also, don't send programs of unknown origin to your friends or family simply because they're funny -- they might contain a virus.

Spoofing: Advances in technology have allowed spammers and malcontents to actually impersonate another person's email address, also known as "spoofing." Email spoofing occurs when an email message looks as if it is from one person, usually someone you know, when it actually was sent from another source. Spoofing is often an attempt to trick you into opening an email attachment that contains a virus; remember that if you weren't expecting an attachment from someone, it is a good idea not to open it.

Social Engineering: Remember that while service providers like America Online may occasionally request that you change your password, they will **not** specify what you should change it to. Also, most legitimate service providers would **never** ask you to send any password information or file via email. If you suspect that you may have received a spoofed email from someone with malicious intent, you should contact your service provider's support personnel immediately. Also, remember that a company will never actually send you a patch for a program via email.

Summary

The safest thing to do when you receive an attachment or file from someone that you're not expecting is to email back that person and ask him if he sent you a file. If he didn't, then delete it. If you receive an attachment from someone you don't recognize at all, don't even think twice and delete the file.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

Information Security Newsletter Series: Spam Email

If you're like most people, you've already encountered problems with Spam email. Spam email is the common term for the Internet version of junk mail. A Spam email is an unsolicited mailing, usually sent to many different people. Spam email comes in many different forms. The most common form is unsolicited (and sometimes offensive) advertising, but spam email also includes chain letters ("pass this email on or you will be jinxed"), hoaxes ("Bill Gates will give you $500 dollars if you forward this email"), scams ("free gutter installation"), and even forwarded jokes. While Spam seems harmless enough, there are actually several reasons why you should be concerned about it.

The first reason is that Spam email costs money. The recipient of the advertising is forced to pay the cost of the message. You pay for email for various reasons, but not to receive unsolicited advertising. Spam email also wastes valuable time, because you have to spend extra time to download the unwanted messages, and then wade through the junk email in order to get to the email you actually want. Have you ever kept track of how much time you spend wading through Spam email? The final reason to be concerned about Spam email is that, if it continues to grow, the costs will continue to rise. ISPs and other businesses spend incredible amounts of money fighting Spam email. If the costs continue to increase, it will most certainly be transferred to the consumer.

So what can you do to help eliminate Spam email? Here are a few tips that you and your family can follow:

- **Don't Give Your Email Address to Websites**. There are many legitimate reasons for giving out your email address, but be aware that many websites use this information to send out advertising. Many websites actually sell your email address to professional spammers.
- **Never Respond to Spam Email**. For a Spammer, one "hit" among thousands of mailings is enough to justify the practice.
- **Never Respond to a "Remove" Reply**. This is just a trick to get you to react to the email -- it alerts the sender that a human is at your address, which greatly increases its value. If you reply, your address is placed on more lists and you receive more Spam email.
- **Never Use Sites that Promise to Remove your Name from Spam Email Lists**. These sites are of two kinds: (1) sincere, and (2) Spam address collectors. The first kind of site is ignored (or exploited) by the Spammers, and they often own the second.
- **Don't Spam**. Sometimes, the best thing you can do to fight Spam email is to make sure you don't do it yourself. Before forwarding on a joke, ask yourself if it is the right thing to do. We all appreciate a good joke, but receiving twenty a week from the same person can get old pretty quickly.
- **Buy a Spam-Blocking Tool**. Recently, several different software packages have surfaced that claim to eliminate Spam email from your inbox. You might try one of these packages, although many of them accidentally get rid of authentic emails from your friends and family.

Unfortunately, Spam email will be around for some time. However, if you and your family follow the tips listed above, you may be able to minimize the number of Spam emails in your inbox.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

Information Security Newsletter Series: Computer Virus Identification and Prevention

Even though new computer viruses are created almost daily, there are practical steps you can take to prevent these viruses. This article will define a computer virus, identify the most common virus sources, highlight the three virus protection steps, and finally explain your role in virus protection.

A computer virus is a software program written to damage other computer programs; some viruses will actually erase everything on your computer, and others will randomly pick a document in your computer and email it to everyone in your address book. Viruses self-replicate and attach themselves to files such as documents, presentations, and system files and can be spread by email, CDs, and floppy disks. Viruses may also infect hardware such as system memory and hard drives.

There are several warning signs associated with viruses. Files that increase in size randomly, the appearance of unknown files, lost files, the inability to save files, corrupted files, sudden lack of hard drive space, the inability to access programs, your system not starting or closing correctly, or strange messages appearing on your screen are all telltale signs that you might have a virus.

Prevention—You must install virus protection software in order to detect, eradicate, and report viruses. There are several programs out on the market, and all are very reasonable in price. It is much cheaper to buy virus prevention software than it is to fix a computer once it's infected. Of course, you also need to update your virus definitions frequently; new viruses are created every day, and it's up to you to make sure that your software is up to date by checking with your anti-virus software's website or running updating software, which will automate the task for you. A final and important step in prevention is to delete email attachments without opening them and to refrain from downloading files from the Internet.

Detection—Installing the program is not enough to prevent viruses. It's up to you to make sure the program is run on a regular basis—twice weekly is usually enough. It's also a good idea to run the program manually on occasion to make sure it is doing its job.

Eradication—When a warning is given about a virus being detected on your computer, you must act quickly and quarantine the virus, delete it, and repair the compromised program; most virus protection programs do this for you.

Following these three simple rules is the best way to prevent your information system from being attacked by viruses. Virus protection software can handle most threats from viruses as long as the software is regularly updated. Anti-virus software relies on people like you to provide information on new viruses so antidotes can be created quickly, and with new viruses being generated daily, it is essential that your virus definitions are up to date.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

Information Security Newsletter Series: Computer Backups

Has it ever happened to you? One minute, you are working on a file on your home computer, and the next minute, you get a blue "error" screen—your hard drive has "crashed." We all hope that computer failure—hard drive and system crashes, blue screens, lost data, and computers that just won't start up—don't happen to us. Unfortunately, they can—and do—happen. Computer failure can be as small an issue as that irritating message that a program is not responding during your shutdown process to losing valuable and often irreplaceable information. Because computer failure is inevitable, you should take measures to prevent the loss of data and files and restore you computer to its original condition. What is this measure? Backup. Backing up your computer involves either copying everything on your computer to another disk or taking a "snapshot" of your computer's data so that it can be rebuilt. While it sounds complicated, it is actually quite easy.

There are two basic back up methods. The first is to use a removable storage device, such as a CD-R drive, an external hard drive, or even floppy disk drive, to manually save the data that is important to you. If you choose this method, you must make sure that you remember to do it often. The second method is to use a software package that will guide you through the back up process to ensure a quality backup. The advantage of this latter method is that, not only will you save all your important files, but you will also have an "image" of your computer that will make it easier for you to get your computer up and running smoothly.

Either way there are a few important things to keep in mind to ensure the best backup possible:

- Backups should be tested for correctness. A test of the backup method should be done with files that are considered disposable. After you perform a backup, you should delete those files from your hard drive and then try to replace them using your backup.
- Backup your computer in several different media forms and make copies of each: Common backup media include: Diskettes, tape, portable storage (i.e. zip disk), CD-R and hard drives. It is always a good idea to make multiple copies in 2 separate locations.
- Backup at least once or twice a month to keep it current and keep your files safe. (If you use your computer for business purposes, you may want to backup at least once every week.
- Run a virus scan on your computer before you backup, and run a virus scan on a backup before restoring it to your computer. Failure to do so will only perpetuate the problem.
- Only backup what is necessary: It is not necessary to backup an entire hard drive. Most computers come with restoration CDs that will help you get your computer back up and running.

It is easy to forget to backup your computer, especially when nothing seems wrong with your computer. However, as many people can tell you, it only takes one hard drive crash with no backups to make you wish you followed this simple practice. Follow the strategies suggested above or look into a software package that automates backups for you to keep your data safe.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

Information Security Newsletter Series: Firewalls

Computer attacks are on the rise, and it makes sense to be concerned about your family's safety while surfing the internet. Unfortunately, many of us have a false sense of security because of the "it won't happen to me" mentality; the truth is that it does happen to ordinary people everyday. Hackers steal identities and wreak havoc on people's private lives. The good news is that there are ways to prevent these attacks.

A first step in protecting your computer and the information stored on it should be to invest in a firewall. A firewall is a piece of software or hardware that works by blocking intruders from gaining access to your PC.

Although a firewall can cost anywhere from $50 - $250 dollars, the benefits of having one greatly outweighs the purchasing cost. This is especially true when the cost of a security breach is factored into the equation. When connected to the Internet, a computer can potentially have 65,535 open "doors," or ports, that are exposed to everyone on the Internet. A firewall will "close" these ports for you and make sure that other computer systems can't "see" your computer. What this boils down to is that it is a lot harder for an unauthorized user, such as a hacker, to access a computer, especially from the outside world. This is especially important for people who use a broadband Internet connection.

While there are benefits of using a firewall, there are also some limitations. Firewalls cannot protect against viruses or worms, so it is important to also install, use, and regularly update anti-virus software. Also, firewalls are like any other piece of computer equipment; they must be maintained. Once you have installed a firewall on your home computer system, it is important to regularly check for software and hardware (also know as "firmware") updates; most firewalls will have a built-in mechanism to do this.

So, what is the best firewall on the market? There are actually many good firewalls out there. It will be well worth your time to use an Internet search engine to do a little bit of consumer research before you make a purchasing decision; take some time to read product reviews from reputable sources. Look for a firewall that monitors incoming and outgoing traffic, and make sure the firewall is user-friendly. Some firewalls come with wizards and helpful configuration screens that will help you make sound decisions about what type of configuration you would like to have, while others are more sophisticated and require more knowledge on your part. A recent trend in firewalls to consider is the bundling of other security features: several firewalls now come with spam filters, pop-up blockers, parental controls, cookie filters, and intrusion detection systems. While these added features may slightly increase the price, you might find them worth the trouble.

With more people falling victim to the increased amount of internet crimes and other malicious activity, it is very important to keep information security a top priority at work and at home. Installing and using a firewall is a good step towards peace of mind and should be part of an overall information security strategy. We'll learn about more steps you can take to protect yourself and your family from online threats in upcoming newsletters.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

Information Security Newsletter Series: Identity Theft

Identity theft, the fastest growing non-violent crime in America, occurs when someone steals another person's personal information—name, social security number, credit card numbers, and so on—and uses it to commit fraud. Identity thieves use this information to open credit card accounts in your name, take out loans, buy cars, establish wireless service, and more—all at no expense to the thief. A person has his or her identity stolen about once every 60 seconds. The information needed to steal a person's identity is acquired by stealing a wallet or mail, rummaging through trash to acquire old credit card or bank statements, or even posing as a landlord or employer to obtain a credit report.

Now that we understand what identity theft is and how it can occur, we can start to think about prevention. There are concrete measures you can take to greatly reduce the risk of becoming one of the 900,000 new victims of identity theft:

1. Use strong passwords for your credit card, bank and phone accounts: Avoid easily guessed passwords such as you Mother's maiden name, a birthday, your address, etc. You can view the Passwords Newsletter for more suggestions.
2. Secure personal information in your home, especially if you live with a roommate.
3. Stay up to date on information security procedures within your workplace.
4. Never give out personal information over the phone, mail, or Internet unless you have initiated contact with that person.
5. Protect information in your mail and trash by shredding credit card applications, bank statements, and anything else that could be used to steal your identity.
6. Carry your Social Security, credit, and bank cards only when necessary. Otherwise, leave them in a secured place.
7. Check your billing statements to look for purchases that you have not made.
8. Periodically check your credit report and rating to look for any malicious activity. Some signs to look for include:
    - Inquiries of your credit report: This will often include requests for credit from employers, collection agencies, or someone else with a legal right to check your credit report.
    - Incorrect address: Thieves will often change billing addresses of accounts you may have and forgotten about. All unused accounts should be closed as soon as possible in all cases.
    - Unexpected public record: This shows court judgments, liens, foreclosures, and other public records. Look for occurrences that you are unaware of or are not yours.
    - Unexpected derogatory information: Look for unexpected past-due items.

If you suspect that you have become a victim of identity theft, you should contact the fraud departments of each of the three major credit bureaus (www. Equifax.com, www.Experian.com, and www.transunion.com), file a police report both with your local police or the police in the community where the identity theft occurred, and close the accounts that you know or believe have been tampered with or opened fraudulently. Your personal information is irreplaceable. By taking the steps mentioned you will have better peace of mind about who is spending your money and using your good name.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

PTA Presentation: Teaching Your Children to Use the Internet Safely and Responsibly

Internet usage continues to escalate, particularly among children. This powerful tool offers many opportunities for recreation, growth, and learning. On the Internet, children can get help with their homework, research topics of interest, take virtual field trips, and communicate easily with pen pals that live thousands of miles away.

However, the internet also presents many security threats to children and to their families. Some of the main threats can be categorized into two groups: privacy and safety issues and inappropriate online behavior.

Privacy and Safety Issues: identity theft, child predation, child harassment, loss of personal files

Inappropriate Online Behavior: unfiltered searches that lead children to offensive material (pornography, hate groups, hacking tools), spam, viruses, theft of copyrighted material

While these threats will always exist, parents can work with their children to reduce the risks of becoming victims—or perpetrator—of cyber crime. This presentation familiarizes parents with information security issues and introduces the idea of creating a contract with their children to help manage their family's use of the Internet. This contract can help protect families against Internet dangers by helping parents communicate with their children about cyber-ethics, cyber-safety, and cyber-security issues. Creation of the contract can also reduce family conflict concerning Internet use by setting clear guidelines for use and establishing consequences for lack of observance of guidelines. Utilizing the defenses of prevention and collaboration, the Internet Use Contract can enable families to use the Internet safely and responsibly.

Delivered by CERIAS personnel experienced in information security issues and K-12 education, this presentation can be modified to fit any specified time frame from 30 minutes to 2 hours. In addition, this presentation is also available in the form of a self-instructional document. For more information, or to schedule a presentation, please contact Teri Schmidt at tmschmid@cerias.purdue.edu or 496-6761.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

Information Security Announcement Series

Purpose

In conjunction with Information Security Awareness Week in April, the Information Security Announcement Series is a list of twenty-four short tips and procedures for effective information security practices to be read with school announcements during either that week or the entire month. They can be read separately or in some sort of themed week format.

To be read each time

April <days> is Information Security Awareness Week, and in observance of this important subject, <school> will present an information security tip each day in order to make your home computer harder for people to steal information from. Today's important tip is in the topic of <topic>:

Passwords

- Always make passwords at least six characters in length and use both letters and numbers when creating them.
- Change your password on a regular basis, but always make sure it's something you can remember and not have to write down.
- Make sure you use a password that you can type quickly without looking at the keyboard, making it harder for someone to steal your password by watching over your shoulder.
- Don't use your login, your own name, your family's names or your pets' names in any form as your password. Also never use publicly accessible information about yourself, such as social security number, license numbers, phone numbers, address, or birthdays.
- Don't use the "Remember Password" function on mail or website browsers. If someone were to steal your computer, it would become that much easier for him to get to all vital information on your system.
- yourself, such as social security number, license numbers, phone numbers, address, or birthdays.
- Don't use the "Remember Password" function. If someone were to steal your computer, it would become that much easier for him to get to all vital information on your system.

Viruses

- A computer virus is a program written specifically to infect and/or alter other programs by self-replicating and attaching themselves to things like documents, presentations, and system files and can be spread by email, CDs, and floppy disks.
- There are three basic steps to computer virus protection. The first is prevention, which is the installation of virus protection software in order to detect, eradicate, and report viruses.
- The second step of computer virus protection is detection, or making sure that once you buy anti-virus software,

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

it is run on a regular basis so computer viruses can be found and destroyed.

- The third step of computer virus protection is eradication. When a warning is given about a virus being detected on your computer, you must act quickly and quarantine the virus, delete it, and repair the compromised program.

Physical Risks

Begin each day with: In addition to the risks associated with connecting your computer to the Internet, there are a number of risks that apply even if the computer has no network connections at all. It is important to note, however, that the ways to reduce these physical risks may also help reduce the chance of online risks.

- Hard drive crashes are a common cause of information loss on personal computers, and regular system backups are the only effective remedy for making sure your information is safe. It's also a good idea to store important information on disks, so if the hard drive does fail, you still have that information stored somewhere else.
- Power problems can also cause physical damage to a computer by inducing a hard drive crash or harming the electronic parts of the computer as well. Common ways of protecting your information system from such threats include using surge protectors and uninterruptible power supplies.
- Physical theft of a computer results in the loss of confidentiality and availability. Although regular system backups allow for recovery of the data, backups alone cannot address confidentiality. Cryptographic tools are available that can encrypt data stored on a computer's hard disk so only those with the correct tools can make the data readable again.
- The older your operating system, like if you're still using Windows 3.1 on your computer, the more likely the chance it's not as secure, which makes it more vulnerable to threats. If someone knows what OS you're running on your computer, the more likely he'll be able to access your system and exploit weaknesses within it. Making sure that you frequently check for security patches and updates will help keep your system more secure.

Computer Ethics

Begin each day with: Just as much as there are rules for saying and doing certain things in the real world, there are rules for conducting yourself in the cyber world. The Computer Ethics Institute has defined The Ten Commandments For Computer Ethics, and today's commandment is:

1. **Thou shalt not use a computer to harm other people.** This would include not just hacking into another computer, but also using websites or email to send out hateful information

about someone else, a school, or place of business.

2. **Thou shalt not interfere with other people's computer work.** This would be any sort of interruption in someone's normal routine online or at his computer. Although you'd probably like to put pop-up ads in this category, you really can't.
3. **Thou shalt not snoop around in other people's files.** Any time you look at someone else's files without probable cause, you're in violation of their right to privacy.
4. **Thou shalt not use a computer to steal.** Never take anything off someone's computer without permission
5. **Thou shalt not use a computer to bear false witness.** Don't use your information system in order to lie about other people or events.
6. **Thou shalt not use or copy software for which you have not paid.** You are permitted to make one copy of a program for personal use, as long as neither the original nor copy will be used at the same time.
7. **Thou shalt not use other people's computer resources without authorization.** Just as your child should ask first before they use someone else's things in the real world, they should ask before they use someone else's space on their computer, their web page, or email.
8. **Thou shalt not appropriate other people's intellectual output.** This will probably be the hardest one on the list to explain to your child. With file sharing programs so abundant and everyone taking advantage of them, it will be difficult to show your child that it's illegal and people suffer from the theft of their property, whether it's a TV or a song.
9. **Thou shalt think about the social consequences of the program you write.** Anything that anyone could potentially see needs to be looked at in terms of whether or not it could hurt others emotionally or threaten someone in some way. Laws in cyberspace apply just as much as they do in the real world, and harassment is harassment anywhere.
10. **Thou shalt use a computer in ways that show consideration and respect.** You should always use your information system in a way that is never harmful to anyone else, whether it's by word or deed.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

Your Family and Internet Safety: Creating a Usage Policy

Introduction

A typical teenage girl, Natalie does well in school, plays clarinet in the school band, and like many girls her age, spends much of her time talking to friends in online chat rooms.

One night, Natalie is using her city's chat room when she gets an instant message from a girl she's never met before. Natalie, knowing full well the dangers of being online, never gives out her last name, her address, pictures of herself, nor her phone number to people she doesn't know online, this stranger included. Her new online friend, however, sends Natalie a picture of herself, and upon seeing that they're about the same age, Natalie's guard comes down a little. The two begin to chat about being in the school band, what grade they're in, and their schools in general. After a short while, Natalie's new online friend says she has to go and that she hopes to talk to her again soon. They say goodbye and Natalie goes back to talking to her friends.

The next afternoon there's a knock at the door of Natalie's house. Natalie's mother opens the door to find a policeman standing there asking to speak with her. He says that last night he spoke with Natalie in an Internet chat room while posing as a teenage girl and asks her mother if she's spoken to her daughter about the dangers of talking to people online. Her mother says that she's told Natalie never to give out her last name, her address, phone number, etc. to anyone she doesn't know. The officer says that Natalie never did give out any of that information, but by finding out what high school she goes to, what grade she's in, and what instrument she plays in the band, he was able to get her last name and address with the help of a school yearbook and a phone book.

… by finding out what high school she goes to, what grade she's in, and what instrument she plays in the band, the officer was able to get her last name and address with the help of a school yearbook and a phone book.

The Internet is, perhaps, one of the greatest inventions of all time. Where else can one find information on the most obscure subject, instantly, from anywhere in the world? It has revolutionized how we as a society educate, do business, and communicate, and as more and more people connect to the Internet on a daily basis, the more we can learn and grow as individuals and as a culture.

However, the Internet has its own dangers and there are people out there who use it for the wrong reasons.

As adults we are able to make our own informed decisions about how to spend our time online, but our children require much more guidance and assistance.

The first thing that comes to mind when thinking of online safety is often protection from offensive websites,. There are over 250 pornographic websites created each day, which adds to the over 75,000 already out there. Besides pornography, there are thousands upon thousands of sites on the Internet that contain hate material directed toward people of different races or religious beliefs or sites that promote violence, terrorism or drug use, with many of these sites instructing readers how to build weapons or make drugs in the privacy of their own homes.

But online safety is about much more than offensive websites. Issues such as identity theft, child predation, and harassment are only a few of the darker aspects of the online age. Perhaps the greatest threat to our daily lives is identity theft. Sometimes through a simple Internet search on Google or Yahoo, one can quickly find a person's full name, home address, phone number, parents' names, social security number, etc., and easily fill out credit card applications or make purchases without their knowledge.

Harassment is also very prevalent online. One out of every five kids using the Internet is approached for sex either by email or through chat rooms and instant messaging, and since teens now spend an average of 8.5 hours a week in chats or using email as opposed to 1.5 hours a week using the Internet for school work, this number will only rise.

Financial threats can also be found online. Yes, identity theft can lead to financial trouble, but don't forget about children with a parent's credit card information! Even if your child doesn't have access to a credit card, there are now Internet services that can be paid through the phone bill, not unlike 1-900 numbers, but far more expensive.

> *While on AOL, not an hour went by when I wasn't sent an annoying instant message from someone asking me how old I am, where I live, what my sexual preference is and so on. From time to time the messages would just be down right disgusting. Consistent harassment was enough to make me change my server. I just wanted more privacy while doing research or writing emails.*
>
> Janna—St. Paul, MN

What to do

The good news about facing the dangers of the Internet is that there are many options out there for dealing with these obstacles. The bad news about facing the dangers of the Internet is that there are many options out there for dealing with these obstacles. It truly is a double-edged sword. There is just so much material and software and myths and lies concerning threats to families while online that it's difficult to make heads or tails out of it.

Luckily the plan of attack for combating the dangers of the online world can be put into two easy categories—prevention and collaboration. Prevention includes the technical and non-technical solutions to the issue of protection, while collaboration is concerned with keeping an open dialogue between parent and child about using the Internet so they feel safe and comfortable to come to you for questions or issues.

__Prevention__ includes the technical and non-technical solutions to the issue of protection, while __collaboration__ is concerned with keeping an open dialogue between parent and child…

Once these two categories have been fully discussed, the information learned from them can be used to create a home Internet usage policy for you and your family, which spells out exactly what can and cannot be done while online and the consequences for not following it fully.

Prevention

There are four main steps when it comes to the prevention of online problems—**building good boundaries, avoiding trouble spots, maintaining oversight,** and **setting a good example**.

The four keys to prevention are __building good boundaries, avoiding trouble spots, maintaining oversight,__ and __setting a good example.__

Building good boundaries is a three-step process. First, it's all about location, location, location. The computer should always be in a high-traffic area of the house and never in the child's bedroom. This way you can casually stroll by and see what your child is up to while online rather than banging on the bedroom door and checking for pornography. If your child constantly minimizes windows as you pass, you know something's up.

The second boundary involves setting time restrictions. Remember that children spend on average 8.5 hours a week in chat rooms or sending email while only spending 1.5 hours doing school work online. Setting consistent time limits and scheduling when your child can be online and for what reason will help make sure your child is online for the right reasons.

The third boundary is a technical one. There are many products out on the market today that can help protect you and your children from many of the dangers of being online, with some being more complicated than others.

On the more inexpensive, non-high-tech side, many of these technological boundaries come with your own Internet service provider (ISP). AOL keyword "parental controls" is a good example of this, which allows you to set specific rules for content, messaging, email, etc. for the whole family. It's also a good idea to have separate email accounts for sending email to

friends and family and for sending email to companies and email lists to help keep the SPAM in one location. There are also family filters on search engines and special search engines just for kids. Yahooligans.com automatically filters out websites of a questionable nature so kids can look up information safely, while lycos.com and google.com have password-protected safeguards that filter out what you specifically tell it to filter out for safer searching.

On the more advanced side of the technological boundary, there are many programs that can be bought today to help assist in filtering content. Remember, however, that these should only be bought in order to assist you in protecting your child, not act as a babysitter. Although seventy-one percent of parents stop supervising Internet use by their kids after age fourteen, seventy-two percent of all net-related missing children are fifteen or older.

It's important that any filtering software you purchase is as customizable to your needs as possible. Look for software that allows you to filter out a variety of website content for your children, block specific newsgroups, email, and unmonitored chat rooms, and manages time spent online.

Although there are many filters on the market today that can protect in many different ways, www.filteringreview.com can help you make better sense of everything that's out there with reviews by people who use the products and lists of what each product includes. It's a great place to start before you head out to the store and buy something that doesn't work as well as you hoped.

Once good boundaries have been established, it's important to still **avoid the trouble spots**. Even if you don't buy filtering software, you can still take steps like having your children avoid unmonitored newsgroups and unfiltered searches. Also make sure they stay out of unmonitored chat rooms and keep themselves from talking to people they don't know on messaging programs.

Maintaining oversight involves checking up on your child's Internet activity once they've stopped using it, which is done through checking the history folder and the cookies of the web browser.

Setting a good example is all about doing as you say *and* as you do. If your child sees you downloading music for free or looking at adult websites or minimizing windows every time they come in the room, they're going to feel that it's alright for them to do just the same.

Collaboration

It's essential that you always keep a dialogue with your child about their use of the Internet, and there are three ways to go about doing this—**open communication, constructive activities,** and **balanced use of time.**

*The three keys to collaboration are **open communication, constructive activities,** and **balanced use of time.***

Open communication involves simply asking what your children do while online, from playing games to working on their homework. Ask your children about whom they talk to while online or send email to, and especially encourage them to always come to you if they have questions or concerns about things that happen while they are online.

Open communication also means talking to teachers and administrators at your child's school as well. Although it seems drastic, remember that student Internet use at school has more than tripled since 1997, meaning that children are more likely to be online at school now than at home, and for longer periods of time. Ask teachers and administrators how much they watch their students to make sure they're not going anywhere they're not supposed to be going or how the Internet is used in classes. Most schools today have a usage policy that they have students and parents sign; ask for one if you haven't seen one or request that one be written up so both you and your child know what is expected of them at school.

Kids are in such a hurry to grow up that they will sometimes pretend to be older than they are when they are online. I worry that this kind of behavior, while normal, could lead to a dangerous or harmful situation down the road.

Michael—Greensboro, NC

Talk with your children about privacy. Explain how no one should be able to know names, addresses, phone numbers, social security numbers, etc., and to always ask you before giving any such information out to anyone while online.

Put it into "real-world" terms—it's no different than walking up to any random person on the street and telling that person your life story.

Sexual harassment and exploitation is a subject that no parent wants to think about, but it's a subject that has to be brought up before something possibly happens. There are three steps to take when confronted with this type of incident. First, it's important to identify the problem. There's a big difference between a fellow student making comments and a sexual predator looking to take pictures, so make sure you know exactly what's going on. Also make sure to tell the child that it's just as important to inform you of SPAM and inappropriate websites as it is to inform you about people on instant messenger and in chat rooms. Once you've determined what happened online, and it's something serious, it should

be reported immediately. Since there is no Internet law enforcement, the first people to contact would be your local police and work from there. After the situation has been dealt with, it's important to conclude with talking with the child about how to avoid such an instance in the future.

Constructive activities take open communication to the next level as you sit down at the computer with your child and show them how to navigate the Internet safely, free from incident. Show them websites that are safe for kids to use as you highlight both good and bad content. Go on virtual field trips with your child so they can learn more about subjects that they're discussing in classes. Work on the family's web page together so they can learn more about web publishing and the mechanics of the Internet—it's best to get children online as soon as they can move a mouse.

I worry that my daughter will learn things like the truth about Santa Claus and other sweet, innocent beliefs that a child loves to experience. I mean, don't get me wrong, I am also worried about the usual internet stalkers and porn, but, if I keep a block on those sites for her and do my part, then, I hope that lessens the chance of her exposure.

Jennifer—Flower Mound, TX

It's always best to remember to keep a **balanced use of time** when it comes to using the Internet in everyday life. Remember that the computer is not a babysitter but a tool. You wouldn't leave your child unattended in the garage while you were doing something else, so why would you leave him sitting alone on a computer? Be sure to remind children that there is an entire world outside the door because it's a little difficult to get exercise and sun while sitting at a computer. Finally, set limits and stand by them. If you tell your child that he can only be online for an hour, then make sure he's only online for an hour.

In order to keep to these rules and combine prevention and collaboration, the best solution is to create a home Internet usage policy.

Creating a home Internet usage policy

When a company wants to make sure their employees are doing what they are supposed to be doing while online at work, they have what is referred to as a usage policy. Similar to a contract, a usage policy states what one should and shouldn't do while online and the consequences for not following that policy.

A home-centered Internet usage policy should be a well-balanced combination of both prevention and collaboration...

This same idea can be used in the home environment as well. A home-centered Internet usage policy should be a well-balanced combination of both prevention and collaboration, which contains

specifics on how the Internet is to be used at home and the results of not following those specifics.

What makes it more difficult for you as a parent is writing this policy in a way appropriate for your children. Kids at different ages use the Internet for different reasons, and it's important that you observe your children as they spend time online to see just what they are using it for.

Even though kids use the Internet for different reasons, the fundamental rules remain the same:

- Never give out **any** type of personal information.
- Always abide by the "Golden Rule" when in chat rooms, talking on instant messenger, or sending email—treat others the way you'd wish to be treated.
- Never meet or call people that you've only ever talked to online without parental permission or supervision.
- Always report suspicious activity to those in authority.
- The prohibition of the viewing of certain websites or going to sites of a questionable nature without parental consent.
- Not purchasing things online without parental consent.
- Setting time limits for using the Internet as play time.
- Never open email attachments you're not expecting because they could contain viruses, whether you know the sender or not.
- Never use file sharing programs because they're both illegal and often rampant with viruses.

Also be sure to include parent responsibilities, such as:

- Asking your children about their online friends and what sites they go to.
- Not to overreact when the child comes to you for help, advice, or concern.
- Setting up time when both of you can use the Internet together.

It's also important to stress that this policy applies to home, school, and at friends' homes.

Once the rules have been laid out, both you and your child should decide upon appropriate consequences for not following the rules. This could include complete prohibition from the computer or the Internet, loss of the use of instant messaging programs or chat rooms, games, etc.

Purdue University ● 656 Oval Drive ● West Lafayette, IN ● 47907-2086
(765) 494-7871 ● Fax (765) 496-3181 ● k-12@cerias.purdue.edu ● www.cerias.purdue.edu

Once you've completed your policy, have both of you sign it and post it in a location near the computer where it can always be seen.

Summary

Although software and policies are certainly helpful in preventing children from participating in questionable activities, they can't fully protect children from all the dangers of the Internet. Children ultimately have to make these decisions on their own, but with good parental guidance and models, the chance of harm coming to either your child or your computer will be greatly reduced.

For further information

To learn more about safely using the Internet, please visit the following websites:

www.cerias.purdue.edu/education/k-12
www.getnetwise.org
www.staysafeonline.info

APPENDIX B:
RELATED MATERIAL FOR GOAL 2

The Center for Education and Research in Information Assurance and Security
Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

K-5 Lessson Plan: Instant Messaging 1

Grade Level: 4-5

Objectives:

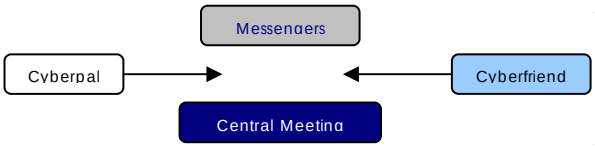
1. Students will learn safe ways to chat and message online.
2. Students will learn that people online may not be who they think that are.

Materials:

Paper, Pens, Envelops

Procedures:

1. Split the students into teams of four or five.
2. Give each team a name. (cyberpal, cyberfriend, cyberbuddy, etc.)
3. Designate one person from each team to be the delivery person.
   a. The job of the delivery person is to deliver a message to another team's messenger at a central meeting place, by quietly calling the other team's messenger over.



4. Designate one person from each team to be the recorder.
   a. The job of the recorder is to write down the team's message.
5. Designate one person from each team who will be sending the message.
   a. The job of this person is to tell the recorder what to write.
6. Designate person(s) from each team to be decoy(s).
   a. The job of this person is to pretend like they are telling the recorder what to write.
7. Instruct the students that they are to send messages to other groups without saying their own name, but only their team name. Only one person from each team will actually tell the recorder what to write. The other person will act as a decoy and give ideas.

> **Cyberpal:** Hello cyberfriend, what is your favorite color?
> **Cyberfriend:** Yellow, what's yours?

8. Allow 5-10 minutes for the students to exchange messages between the different teams. Remind students to keep quiet so that the other teams do not know which student is the real one and which one is the decoy.
9. During the exchange of each message, each team is required to correctly use two terms in context from their current vocabulary or spelling list. If a team fails to use two terms in each message correctly they must use four terms correctly in their next message.
10. Remind students not to tell their age, height, gender, or any personal information about themselves that would give away their identities.
11. After the students have finished giving and receiving messages for a period, have the students, guess who told the recorder what to write for each group. Students must be able to support their answer.
12. Write the students guesses for each group on the chalkboard. Point out any discrepancies between what the different groups thought. For example: *The cyberpal group may have thought that Tim told the recorder what to write for the cyberfriend group, but the cyberbuddy group may have thought it was Anne.*

Closing:

Discuss with students that people online may not be who they think they are. Explain to students that it is easy for somebody to pretend to be somebody else and that is why students should only talk to friends and family that they know online. Explain to students that talking to a stranger on the Internet is no different than talking to a stranger in real life.

Supplemental Reading:

- Girard L.W. (1993) *Who is a Stranger and What Should I Do?* Albert Whitman Press
- Fitts S. (1999) *A Stranger in The Park.* Agreka Books, LLC
- Kevi (2003) *Don't Talk to Strangers* (Hipkidhop Series). Scholastic, Inc. (Includes CD)

Supplemental Websites:

- www.getnetwise.org
- http://www.getnetwise.org/safetyguide/tips/kids.php
- http://www.safekids.com/kidsrules.htm

Indiana Academic Standards:

Grade 4:

Language Arts:

4.1.5 Use a thesaurus to find related words & ideas.

4.1.6 Distinguish and interpret words with multiple meanings (*quarters*) by using context clues (the meaning of the text around a word).

4.5.5 Use varied word choices to make writing interesting.

4.5.6 Write for different purposes (information, persuasion) and to a specific audience or person.

Mathematics:

4.7.1 Analyze problems by identifying relationships, telling relevant from irrelevant information, sequencing and prioritizing information, and observing patterns.

Science:

4.2.5 Write descriptions of investigations, using observations and other evidence as support for explanations.

Grade 5:

Language Arts:

5.5.5 Use varied word choices to make writing interesting.

5.5.6 Write for different purposes and to a specific audience or person, adjusting tone and style as appropriate.

5.6.1 Identify and correctly use prepositional phrases (*for school* or *In the beginning*), appositives (*We played the Cougars, the team from Newport*), main clauses (words that express a complete thought), and subordinate clauses (clauses attached to the main clause in the sentence).

5.6.7 Spell roots or bases of words, prefixes (*understood/misunderstood, excused/unexcused*), suffixes (*final/finally, mean/meanness*), contractions (*will not/won't, it is/it's, they would/they'd*), and syllable constructions (*in-for-ma-tion, mol-e-cule*) correctly.

Instant Message 2: Private Information

Grade Level: 4-5

Objectives:

1. Students will learn what information should be shared over the Internet and what should not be.
2. Students will know what to do when asked for information that they know should not be told over the Internet.

Materials:

- Paper, Pens, Envelops

Procedures:

1. Instruct students to get into their groups as they did for the "Instant Message 1" activity.
2. Instruct the students to switch roles so that everyone has a different role than they did before and a new person is the decoy.
3. This time give each of the groups a card that has a specific piece of information that they are trying to get from the other groups.
   a. What type of shoes are you wearing?
   b. Are you a boy or a girl?
   c. What is your last name?
   d. What color is your shirt?
   e. Are you right or left handed?
4. Allow time for the students to exchange messages, reminding them that only the messengers can exchange at the central meeting place.
5. After the students have finished exchanging the messages, ask the groups who got their question answered by the other groups.
6. Then ask the students whom they think the student was who told the recorder what to write. More answers will be correct.

Closure:

Discuss with students why it was easier to find out who the person was this time. *Knew more personal information about the other groups' person than before.* Discuss with students why it is important not to give personal information online. *You don't know for sure whom you are talking to. Some information is not intended for others to know.* Compose a list of things that should not be told online or lists of questions that you should not answer. Then discuss what should be done if somebody asks you these questions. *Tell an adult that you know and trust.*

Websites that can help to produce lists:

(These websites contain information in which students can learn safe guidelines that they should follow while on the Internet.)

- www.getnetwise.org
- http://www.getnetwise.org/safetyguide/tips/kids.php
- http://www.safekids.com/kidsrules.htm

Extension Activity:

Have each group make a poster that lists things that should not be told online and questions that should not be answered. Display these posters near the computers.

Indiana Academic Standards:

Grade 4:

Language Arts:

4.1.5 Use a thesaurus to find related words and ideas.

4.1.6 Distinguish and interpret words with multiple meanings (*quarters*) by using context clues (the meaning of the text around a word).

4.5.5 Use varied word choices to make writing interesting.
4.5.6 Write for different purposes (information, persuasion) and to a specific audience or person.

Mathematics:
4.7.1 Analyze problems by identifying relationships, telling relevant from irrelevant information, sequencing and prioritizing information, and observing patterns.
Science:
4.2.5 Write descriptions of investigations, using observations and other evidence as support for explanations.

Grade 5:

Language Arts:

5.5.5 Use varied word choices to make writing interesting.
5.5.6 Write for different purposes and to a specific audience or person, adjusting tone and style as appropriate.
5.6.1 Identify and correctly use prepositional phrases (*for school* or *In the beginning*), appositives (*We played the Cougars, the team from Newport*), main clauses (words that express a complete thought), and subordinate clauses (clauses attached to the main clause in the sentence).
5.6.7 Spell roots or bases of words, prefixes (*understood/misunderstood, excused/unexcused*), suffixes (*final/finally, mean/meanness*), contractions (*will not/won't, it is/it's, they would/they'd*), and syllable constructions (*in-for-ma-tion, mol-e-cule*) correctly.

Computer Ethics 1

Grade Level: 3-5

Objectives:

1. Students will be able to recognize which uses for the computer are appropriate.
2. Students will be able to recognize which uses for the computer are not appropriate.
3. Students will be able to recognize why some uses for the computer are not appropriate.
4. Students who improper use of the computer hurts?
5. Students will be able to recognize when others are doing wrong.

Materials:

1. Worksheet for lists of computer uses.

Procedure:

1. Hand out worksheet in which students will list the ways in which they use the computer.
2. Compile a list of all students' responses on the overhead or chalkboard. (Do not write duplicates)
3. Discuss the ways in which each of the things should be used.
4. Ask students to write on the activity sheet ways in which they have seen things listed used improperly.
5. Go through the 10 Commandments of Computer Ethics with students.
6. Have the students discuss why each of these is wrong.

Closing:

Have a classroom discussion about why it is wrong to use things improperly. Discuss who is hurt by improper use of the computer.

Relate the computer to real life, "If you wouldn't do it in the actual world, why would you do it in the cyber world?"

Supplemental Material: Ten Commandments for Computer Ethics, from the Computer Ethics Institute

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people's computer work.
3. Thou shalt not snoop around in other people's files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not use or copy software for which you have not paid.
7. Thou shalt not use other people's computer resources without authorization.
8. Thou shalt not appropriate other people's intellectual output.
9. Thou shalt think about the social consequences of the program you write.
10. Thou shalt use a computer in ways that show consideration and respect.

Indiana Academic Standards:

Grade 3:

Language Arts:

3.2.2 Ask questions and support answers by connecting prior knowledge with literal information from the text.

3.25 Distinguish the main idea and supporting details in expository (informational) text.

3.7.2 Connect and relate experiences and ideas to those of a speaker.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

Grade 4:

Language Arts:

4.2.1 Use the organization of informational text to strengthen comprehension.

4.7.2 Summarize major ideas and supporting evidence presented in spoken presentations.

Social Studies:

4.5.1 Identify ways that social groups influence individual behavior and responsibilities.

4.5.6 Investigate the contributions and challenges experienced by people from various cultural, racial, and religious groups in Indiana during different historical periods by reading biographies, historical accounts, stories, and electronic media, such as CD-ROMs and Web sites.

Grade 5:

Language Arts:

5.2.3 Recognize main ideas presented in texts, identifying and assessing evidence that supports those ideas.

5.2.4 Draw inferences, conclusions, or generalizations about text and support them with textual evidence and prior knowledge.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

Computer Ethics 2

Grade Level: 3-5

Objectives:
1. Students will learn that others' property on the computer is the same as others' property in real life.
2. Students will recognize that they should respect others' property on the computer.

Materials:
1. Computer Disk with Teachers name on it
2. Computer
3. Teacher's desk
4. Pencil sharpener
5. Other materials in which the students may or may not have to asked permission to use
6. Red paper stop signs
7. Green Circles

Procedures:
1. Have students bring in something that is special to them to share with the class.
2. Prepare objects in the classroom in which the students can access without asking for permission.
3. Discuss with the students the difference between the two types of objects. (Student objects and teacher objects)
4. Ask students what they would have to do if they wanted to see or use another student's object.
5. Ask the students what they would have to do if they wanted to see or use the teacher's objects.
6. Discuss the difference between the two.
7. Distribute red stop signs and green circles
8. Instruct students to put the red stop signs next to objects that they think they should ask permission before using and the green circles next to objects that are okay to use without asking for permission.
9. Count the red stop signs and green circles for each object.
10. Put the total number of each green circle for each object on the board.

Closing:
Discuss with the students why they put different colors on different items. Discuss with the students what others peoples property is and how it applies the same way to things on the computer such as, others files, the classroom computer, the printer, etc. Read to students Fables from the Sea, read the story about the seabird learning to respect others property. Have students write the ways in which the seabird learned to respect others property from the sea is similar to the way people must learn to respect others property on the computer.

Supplemental Material:
Hayashi, L. A. (2000). *Fables from the Sea.* University of Hawaii Press

Indiana Academic Standards:

Grade 3:
Language Arts:

3.2.2 Ask questions and support answers by connecting prior knowledge with literal information from the text.

3.2.5 Distinguish the main idea and supporting details in expository (informational) text.

3.7.2 Connect and relate experiences and ideas to those of a speaker.

Grade 4:
Language Arts:

4.2.1 Use the organization of informational text to strengthen comprehension.

4.7.2 Summarize major ideas and supporting evidence presented in spoken presentations.

Social Studies:

4.5.1 Identify ways that social groups influence individual behavior and responsibilities.

4.5.6 Investigate the contributions and challenges experienced by people from various cultural, racial, and religious groups in Indiana during different historical periods by reading biographies, historical accounts, stories, and electronic media, such as CD-ROMs and Web sites.

Grade 5:

Language Arts:

5.2.3 Recognize main ideas presented in texts, identifying and assessing evidence that supports those ideas.

5.2.4 Draw inferences, conclusions, or generalizations about text and support them with textual evidence and prior knowledge.

Computer Ethics 3: Mock Trial

Grade Level: 4-5

Objectives:

1. Students will be able to recognize why it is important to respect others property on the computer.
2. Students will recognize that even if they didn't access information in an illegal way it is still wrong to look at it.

Materials:

1. Packet for defense lawyers.
2. Packet for prosecution.
3. Packet for defendant.
4. Packet for accuser.

Overview of Trial:

The defendant went to a computer in which the accuser forgot to sign off. The defendant looked on the computer at some of the accuser's files. The defendant claims he or she did nothing wrong because the accuser forgot to log out therefore allowing anyone to come up to the computer and look at his or her files.

Procedure:

1. Distribute packet to two lawyers, two prosecutors, one defendant, and one accuser.
2. All the other students will be the jury for the mock trial.
3. The teacher is the judge for the mock trial.
4. Each side makes an opening statement.
5. Have prosecution present their case calling the accuser to the stand.
6. First have the prosecution ask questions to the accuser, then the defense.
7. Have the defense present their case calling the defendant to the stand.
8. First have the defense ask questions to the defendant, then the prosecution.
9. Allow time for the jury to discuss and come up with a verdict.
10. Each side gives a closing statement.

Closing:

If the jury comes up with a verdict in which the defendant is innocent review previous ethics lessons. If jury comes up with a guilty verdict discuss what the defendant should have done upon coming up to a computer in which somebody forgot to log out. (Tell the student, tell the teacher.)

Supplemental Materials:

Description of roles for prosecutors, defense lawyers, defendant, and plaintiff:

Defense Lawyers: Opening Statement:

1. The defendant did not illegally access the accuser's files by stealing a password.
2. It is the accusers fault for not logging out.

Defense Lawyers: Questions for Accuser:

1. If you cared about your files so much why didn't you log out?
2. Don't you think that it is disrespectful to other students that you did not log out?

Defense Lawyers: Questions for Defendant:

1. Did you use the accuser's password to access the computer?
2. Whose fault do you think it is that the accuser's files were accessed?
3. Would you have ever seen the accuser's files if he or she would have logged out properly?

Defense Lawyers: Closing Statement:

1. The defendant did nothing wrong because he did not steal the password to access any of the files.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

Prosecutors: Opening Statement:
1. Nobody should ever look at another person files without permission.
2. The accuser made an honest mistake by forgetting to log out, and the defendant should have told
him or her about it.

Prosecutors: Questions for Accuser:
1. Why didn't you log out?
2. What do you think the defendant should have done when they came across your files?

Prosecutors: Questions for Defendant:
1. Why didn't you tell the accuser when he or she forgot to log out?
2. How would you feel if somebody looked through your files?

Accuser:
You feel that you did nothing wrong and that the defendant should have told you about you forgetting to log out. You also feel that nobody should ever look at anyone else's files.

Defendant:
You feel like the accuser should have remembered to log out. If the accuser cared about his or her files that much they would have made sure to log out of the computer. You didn't illegally access through stealing a password. You feel like you did nothing wrong.

Indiana Academic Standards:

Grade 4:

Language Arts:

4.7.1 Ask thoughtful questions and respond orally to relevant questions with appropriate elaboration.
4.7.5 Present effective introductions and conclusions that guide and inform the listener's understanding of important ideas and details.
4.7.6 Use traditional structures for conveying information, including cause and effect, similarity and difference, and posing and answering a question.
4.7.7 Emphasize points in ways that help the listener or viewer to follow important ideas and concepts.
4.7.8 Use details, examples, anecdotes (stories of a specific event), or experiences to explain or clarify information.

Social Studies:
4.2.6 Give examples of how citizens can participate in their state government.
4.2.7 Define and provide examples of civic values in a democracy.

Grade 5:

Language Arts:
5.7.1 Ask questions that seek information not already discussed.
5.7.3 Make inferences or draw conclusions based on an oral report.
5.7.4 Select a focus, organizational structure, and point of view for an oral presentation.
5.7.5 Clarify and support spoken ideas with evidence and examples.
5.7.6 Use volume, phrasing, timing, and gestures appropriately to enhance meaning.

Passwords 1: Role of Passwords

Grade Level: 4-5

Objectives:

1. Students will learn the role passwords play in protecting information.

Materials:

Team Secret Information Cards

Procedures:

1. Split the classroom into four teams. Tell the students that they are competing companies who are trying to build the first "Hover Craft Car" for families to use. Each group has one of four parts to the design of the "Hover Craft Car". They need to find out the others plans in order to complete their design.
2. The teams will all be distributed four cards that have their team name and secret design. (The teams each have four cards in case more than one team successfully accesses their information)
   a. Hover Builders and Co.
   b. Hover Car Inc.
   c. Flying Vehicles Inc.
   d. The Hover Craft Company
3. Distribute to each team the secret plans that they are to protect. The only way for anyone to see the secret plans is to enter the password. The classroom teacher acts as the login station and allows only the people who have the correct password to view the plans.
4. Have students work in their group to come up with a four part password that uses only the numbers, "1, 2, 3, and 4." Using each number only once in their password. (Example: 3214)
5. Once the students have come up with their password they turn in a sheet of paper to the teacher that has their team name and password on it. The students also turn in their secret plan for the teacher to protect.
6. Tell students that their goal now is to try and figure out the other companies' passwords and attempt to access their information. Explain to students that in order to access information they must say the company name and then write the company's correct password and hand the password to the teacher.

Hover Builders and Co. Password:

?	?	4	?
___	___	___	___

7. If a team attempts to access another team's password but guesses incorrectly one number of their password in its correct position is written on the board for the other teams to see. Inform teams that they should be careful before attempting to access another team's information and to keep track of the access attempts that they make for each team.
8. Allow the teams to do the activity until one team has successful accessed all the other teams' information.

Closing:

Discuss with the students the role that passwords played in this activity. How did passwords successfully stop intruders from seeing the valuable information of your company? What ways types of information could a password protect?

Indiana Academic Standards:

Grade 4:

Language Arts:

4.7.1 Ask thoughtful questions and respond orally to relevant questions with appropriate elaboration

Math:

4.6.1 Represent data on a number line and in tables, including frequency tables.

4.6.2 Interpret data graphs to answer questions about a situation.

4.6.3 Summarize and display the results of probability experiments in a clear and organized way.

4.7.1 Analyze problems by identifying relationships, telling relevant from irrelevant information, sequencing and prioritizing information, and observing patterns

4.7.8 Make precise calculations and check the validity of the results in the context of the problem

4.7.9 Decide whether a solution is reasonable in the context of the original situation.

4.7.10 Note the method of finding the solution and show a conceptual understanding of the method by solving similar problems.

Grade 5:

Language Arts:

5.7.5 Clarify and support spoken ideas with evidence and examples.

Math:

5.7.3 Apply strategies and results from simpler problems to solve more complex problems.

5.7.4 Express solutions clearly and logically by using the appropriate mathematical terms and notation. Support solutions with evidence in both verbal and symbolic work.

5.7.8 Decide whether a solution is reasonable in the context of the original situation.

5.7.9 Note the method of finding the solution and show a conceptual understanding of the method by solving similar problems.

5.6.3 Understand that probability can take any value between 0 and 1, events that are not going to occur have probability 0, events certain to occur have probability 1, and more likely events have a higher probability than less likely events.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

Team Identification Cards:

Hover Builders and Co. Password: _____

Your company has figured out how to make the "Hover Craft" float in the air. Come up with a password and then return this card back to the teacher. Remember your password can only have the numbers 1-4 using each number only one time.

After giving the teacher your password try and figure out the other teams passwords. Remember if you guess incorrectly a portion of your company's passwords will be shared with the other companies.

Hover Car Inc. Password: _____

Your company has figured out how to make the "Hover Craft" move forward. Come up with a password and then return this card back to the teacher. Remember your password can only have the numbers 1-4 using each number only one time.

After giving the teacher your password try and figure out the other teams passwords. Remember if you guess incorrectly a portion of your company's passwords will be shared with the other companies.

The Hover Craft Company Password: _____

Your company has figured out how to make the "Hover Craft" move backwards. Come up with a password and then return this card back to the teacher. Remember your password can only have the numbers 1-4 using each number only one time.

After giving the teacher your password try and figure out the other teams passwords. Remember if you guess incorrectly a portion of your company's passwords will be shared with the other companies.

Flying Vehicles Inc. Password: _____

Your company has figured out how to make the "Hover Craft" stop once it is moving. Come up with a password and then return this card back to the teacher. Remember your password can only have the numbers 1-4 using each number only one time.

After giving the teacher your password try and figure out the other teams passwords. Remember if you guess incorrectly a portion of your company's passwords will be shared with the other companies.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

Passwords 2: Making Good Passwords

Grade Level: 4-5

Objectives:

1. Students will learn how to make good passwords.

Materials:

Team Identification Cards, information on how to write a good password.

Introduction:

Discuss with the students why it was easy for the other companies to figure out their passwords in the first Password Activity. The passwords were all very simple and contained only four different characters.

Activity:

1. Have the students return back to their groups.
2. This time have the groups create a new password that contains at least eight characters. Instruct the students to make sure that there is at least one character that is not a letter, either a number or some type of punctuation mark. Instruct the students that they should also include some capital and lowercase letters in their password.
3. Have the students complete the activity as they did in Passwords.
4. For each incorrect guess the teacher still puts a portion of that team's password up on the board to share with the other companies.
5. After one or more team has completed the activity have a discussion with the students.

Closing:

Discuss with the students why this time it was much harder to access the other teams' secret information. What changes in the activity made it more difficult to figure out the other teams' passwords. Construct a list on the board of ways to create a "good password," and what things not to include in a password. Remind students that it is also good to change passwords on a regular basis, and not to use personal information in the passwords. Discuss with students why to use different characters and how the more characters you use and the number of characters in each password affects how easy it is to crack.

Possible Password Combinations:

Possible Characters in Password	Number of Characters in Password	Formula	Number of Possible Password Combinations
0-9	4	10^4	**10,000**
0-9	8	10^8	**100,000,000**
0-9 & 26 letters	4	36^4	**1,679,616**
0-8 & 26 letters	8	36^8	**2,821,109,907,456**

How to Write a Good Password:

The following are ten tips to help you select a password that is more secure, yet still relatively easy for you to remember.

1. Use a minimum of 6 characters.
2. Use a combination of numbers (1-9), alphanumeric characters (A-Z), and special characters (!, @, #, $, %, ^, &,*,+,=).
   Try this on for size: Get>Sm@rt
   If it is hard for you to remember special characters, create a common substitute that makes sense to you. For example, use $ as a substitute for s or S. Or use + as a substitute for t or T.
   So instead of Get>Sm@rt, the password could be Ge+>$mar+
3. Don't pick a password that someone can easily guess. What types of things are easy to guess? Here's a list of things that we advise you not use because they are easy to guess.
   - Don't use your login name in any form (as-is, reversed, capitalized, doubled, etc.).
   - Don't use your first or last name in any form.
   - Don't use your spouse's or child's name.
   - Don't use other information easily obtained about you. This includes license plate numbers, telephone numbers, social security numbers, the brand of your automobile, the name of the street you live on, etc.
   - Don't use a password of all digits, or all of the same letter. This significantly decreases the search time for a cracker.
   - Don't use a word contained in (English or foreign language) dictionaries, spelling lists, or other lists of words.
4. Use a pass phrase. A pass phrase is sort of like a personal algorithm. The phrase makes it easy for you to remember, but hard for someone else to guess.
   For example: The title of the song I Left My Heart in San Fransisco is a phrase that could be represented as the following password:
   EYELMHISF
   If you like the idea of using personal information in a pass phrase, consider the following passwords:
5. Use a separate password for different accounts. I know this makes it tough to remember multiple passwords. Try associating the password with the account. If you have an account to purchase books on line, use a pass phrase that is derived from a book title. For example: Using the book title The Seven Habits of Highly Effective People could result in the following password: 7Hof^EP!
6. Do not write down your password and leave it in an easy to view spot. There isn't much else to say here…..just don't do it.
7. Change your password regularly. There is a temptation to recycle old passwords. You have two and you flip flop their use. Resist the temptation….it is too predictable.
8. Do not give other people your password, intentionally or unintentionally. While it might seem efficient to give your colleague your password so s/he can get a file off of your computer, who is to say that they will not write it down somewhere for ease of remembering. You also want to make sure that it is difficult for others to see you type in your password.

9. Use the timeout feature to prohibit access when you are away from your desk.
10. Report any suspicious or abnormal circumstances to your system administrator as soon as you notice it.

Supplemental Materials:

http://itim.tamu.edu/good_passwords.shtml
This website will provide teachers with information on how to write a good password.

Indiana Academic Standards:

Grade 4:

Language Arts:

4.7.1 Ask thoughtful questions and respond orally to relevant questions with appropriate elaboration.

Math:

4.6.1 Represent data on a number line and in tables, including frequency tables.

4.6.2 Interpret data graphs to answer questions about a situation.

4.6.3 Summarize and display the results of probability experiments in a clear and organized way.

4.7.1 Analyze problems by identifying relationships, telling relevant from irrelevant information, sequencing and prioritizing information, and observing patterns

4.7.8 Make precise calculations and check the validity of the results in the context of the problem.

4.7.9 Decide whether a solution is reasonable in the context of the original situation.

4.7.10 Note the method of finding the solution and show a conceptual understanding of the method by solving similar problems.

Grade 5:

Language Arts:

5.7.5 Clarify and support spoken ideas with evidence and examples.

Math:

5.7.3 Apply strategies and results from simpler problems to solve more complex problems.

5.7.4 Express solutions clearly and logically by using the appropriate mathematical terms and notation. Support solutions with evidence in both verbal and symbolic work.

5.7.8 Decide whether a solution is reasonable in the context of the original situation.

5.7.9 Note the method of finding the solution and show a conceptual understanding of the method by solving similar problems.

5.6.3 Understand that probability can take any value between 0 and 1, events that are not going to occur have probability 0, events certain to occur have probability 1, and more likely events have a higher probability than less likely events.

Team Identification Cards:

Hover Builders and Co. Password: _____

Your company has figured out how to make the "Hover Craft" float in the air. Come up with a password and then return this card back to the teacher. Remember your password can only have the numbers 1-4 using each number only one time.

After giving the teacher your password try and figure out the other teams passwords. Remember if you guess incorrectly a portion of your company's passwords will be shared with the other companies.

Hover Car Inc. Password: _____

Your company has figured out how to make the "Hover Craft" move forward. Come up with a password and then return this card back to the teacher. Remember your password can only have the numbers 1-4 using each number only one time.

After giving the teacher your password try and figure out the other teams passwords. Remember if you guess incorrectly a portion of your company's passwords will be shared with the other companies.

The Hover Craft Company Password: _____

Your company has figured out how to make the "Hover Craft" move backwards. Come up with a password and then return this card back to the teacher. Remember your password can only have the numbers 1-4 using each number only one time.

After giving the teacher your password try and figure out the other teams passwords. Remember if you guess incorrectly a portion of your company's passwords will be shared with the other companies.

Flying Vehicles Inc. Password: _____

Your company has figured out how to make the "Hover Craft" stop once it is moving. Come up with a password and then return this card back to the teacher. Remember your password can only have the numbers 1-4 using each number only one time.

After giving the teacher your password try and figure out the other teams passwords. Remember if you guess incorrectly a portion of your company's passwords will be shared with the other companies.

Software Theft

Grade Level: 4-5

Objectives:

1. Students will learn that copying software no different than stealing from a store.

Materials:

Student scripts, mock classroom store.

Procedures:

1. Set up a classroom store that contains computer programs.
2. Next distribute the roles that some students in the classroom are to play in two short skits.
3. Give time for the students who are involved to practice/memorize their roles in the skits.
4. Act out the first skit, "Stealing from a Store."
5. Have a classroom discussion in which the students answer the following questions.
   a. Who was hurt by theft that they witnessed?
      i. Consumers, business owners, the person who stole.
   b. How are each of these people hurt?
   c. What happens as a result of this person stealing?
6. Act out the second skit, "Copying a Program from A Friend."
7. Have a classroom discussion in which the students answer the following questions.
   a. Who was hurt by what they witnessed?
      i. Consumers, business owners, the person who stole.
   b. How are each of these people hurt?
   c. What happens as a result of this person stealing?

Closing:

Discuss with the students that copying a program from a friend is no different than stealing directly from a store. Also discuss with the students that stealing from an unknown person on the internet is no different that stealing from a friend or directly from a store. Downloading music from the Internet is also stealing.

Extension Activity:

Have students develop skits that show how downloading music from the Internet and stealing from an unknown person on the Internet is also stealing. Have the students show who is hurt by these types of theft.

Indiana Academic Standards:

Grade 4:

Language Arts:

4.3.3 Use knowledge of the situation, setting, and a character's traits, motivations, and feelings to determine the causes for that character's actions.

4.7.6 Use traditional structures for conveying information, including cause and effect, similarity and difference, and posing and answering a question.

4.7.7 Emphasize points in ways that help the listener or viewer to follow important ideas and concepts.

4.7.9 Engage the audience with appropriate words, facial expressions, and gestures.

Grade 5:

Language Arts:

5.7.1 Ask questions that seek information not already discussed.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

5.7.3 Make inferences or draw conclusions based on an oral report.
5.7.4 Select a focus, organizational structure, and point of view for an oral presentation.
5.7.5 Clarify and support spoken ideas with evidence and examples.
5.7.6 Use volume, phrasing, timing, and gestures appropriately to enhance meaning.

Roles for Skit One: "Stealing from a Store"

Thief: You enter the store and start looking around. You find a game that you really want to play on your computer. You ask the Cashier how much the game is. The Cashier tells you that it is $35. You don't have that much money so you continue to browse the store to try and find a cheaper game. You cannot find a cheaper game that you want to play. You decide that because the store is pretty empty and the Cashier and Store Owner are busy helping other customers you should just take the game and leave the store without being caught.

Store Owner: You are busy working at your store. You are too busy helping another customer in the store to notice that the Thief had stolen the game. That night after all of the customers have left you notice that the game is missing. You ask the Cashier if he/she sold the game during the day. The cashier tells you, "no." Not being able to afford the lost money from the stolen game you make the prices of all the other games more expensive to make up for the money that you lost because of the stolen game.

Cashier: You help the Thief when he enters the store. You tell the Thief the price of the game ($35) and ask the Thief if they want to buy the game. When the Thief says, "No," you help another customer who was in the store. After all the customers have left the Store Owner asks you if you sold the game during the day. You tell the Store Owner, "No."

Store Customer 1: You are in the store you find a program that you want to buy and purchase it. You do not notice the Thief stealing the game.

Store Customer 2: You are in the store you find a program that you want to buy and purchase it. You do not notice the Thief stealing the game.

Roles for Skit 2: "Copying a Program from a Friend"

Friend 1: You and your friend are at your house playing a video game that you got for your birthday. It is the newest and most fun game out there. Your friend's mom calls and he/she has to go home. Your friend asks you if you can make a copy of the game so he can play it when he gets home. You decide to make a copy for your friend and he/she takes the game home.

Friend 2: You are over at your friend's house playing a video game on his computer that he got for his birthday. Your birthday is not coming up for six months and you know your parents would never buy the game for you. Your mom calls and tells you that you have to come home. You want to play the game when you get home so you ask your friend to make a copy. Your friend makes the copy and you go home and play it.

Viruses

Grade Level: 4-5

Objectives:
1. Students will learn what computer viruses are.
2. Students will learn how computer viruses can be transferred.
3. Students will learn how to protect themselves from computer viruses.

Materials:
Envelopes, small pieces of paper with sentences that use the weeks spelling words

Introduction:
Ask the students the following questions:
1. What is a virus?
2. How are viruses transferred?
3. What happens when a computer gets a virus?
4. What are some ways in which we prevent from getting viruses?

Activity:
1. Have the students sit in a circle on the floor.
2. Pass around an envelope containing messages on them. Have one message that has virus written on it.
3. After each student has a piece of paper with a message on it, and one person has a piece of paper with the virus on it, the students pick a person across the circle in which they want to give their message too.
4. A basket is passed from the first person who is sending the message to the person across the circle. Each person between the sender and the receiver places their message in the basket along with the original senders.
5. If the person who has the virus message is sitting between the sender and the receiver, when the basket gets to virus holder they put their card in the basket as well.
6. If a basket reaches the receiver without the virus being in there, the receiver reads all of the messages.
7. If the basket reaches the receiver with the virus card in there, the receiver begins reading the messages until they get to the virus card. The virus card stops the rest of the messages from being received.
8. After the receiver has read all he or she can. Fold the messages and redistribute. Choose a new sender and receiver.
9. Repeat the activity so that the message has made it both "infected" and with out being "infected."

Closing:
Discuss with the students that viruses are transferred on the computer through messages that are sent from people. Discuss with the students that they can also get computer viruses from downloading programs in which they don't know where the information is from. Discuss with the students that the virus as it was received affected the receiver, as a virus on the computer affects the receiving computer.

Tell the students ways in which they can protect themselves from getting computer viruses.
1. Do not download programs from the internet without asking your parents first.
2. Do not open emails that have attachments unless you know who the email is from and what the attachment is.
3. Do not accept files through instant messenger unless you know who is sending it and what it is.
4. Do not open files on disk unless you know exactly what is on that disk.

Indiana Academic Standards:

Grade 4:

Language Arts:

4.1.6 Distinguish and interpret words with multiple meanings (*quarters*) by using context clues (the meaning of the text around a word).

4.4.10 Review, evaluate, and revise writing for meaning and clarity.

4.4.11 Proofread one's own writing, as well as that of others, using an editing checklist or set of rules, with specific examples of corrections of frequent errors.

4.4.12 Revise writing by combining and moving sentences and paragraphs to improve the focus and progression of ideas.

4.6.2 Use simple sentences (Dr. Vincent Stone is my dentist.) and compound sentences (His assistant cleans my teeth, and Dr. Stone checks for cavities.) in writing.

4.6.3 Create interesting sentences by using words that describe, explain, or provide additional details and connections, such as adjectives, adverbs, appositives, participial phrases, prepositional phrases, and conjunctions.

4.6.5 Use parentheses to explain something that is not considered of primary importance to the sentence, commas in direct quotations (He said, "I'd be happy to go."), apostrophes to show possession (Jim's shoes, the dog's food), and apostrophes in contractions (can't, didn't, won't).

4.6.8 Spell correctly roots (bases of words, such as *unnecessary, cowardly*), inflections (words like *care/careful/caring*) or words with more than one acceptable spelling (like *advisor/adviser*), suffixes and prefixes (*-ly, -ness, mis-, un-*), and syllables (word parts each containing a vowel sound, such as *sur-prise* or *e-col-o-gy*).

Grade 5:

Language Arts:

5.6.7 Spell roots or bases of words, prefixes (*understood/misunderstood, excused/unexcused*), suffixes (*final/finally, mean/meanness*), contractions (*will not/won't, it is/it's, they would/they'd*), and syllable constructions (*in-for-ma-tion, mol-e-cule*) correctly.

5.6.6 Use correct capitalization.

5.6.3 Identify and correctly use appropriate tense (present, past, present participle, past participle) for verbs that are often misused (lie/lay, sit/set, rise/raise).

5.6.4 Identify and correctly use modifiers (words or phrases that describe, limit, or qualify another word) and pronouns (he/his, she/her, they/their, it/its).

5.6.5 Use a colon to separate hours and minutes (12:20 a.m., 3:40 p.m.) and to introduce a list (Do the project in this order: cut, paste, fold.); use quotation marks around the exact words of a speaker and titles of articles, poems, songs, short stories, and chapters in books; use semi-colons and commas for transitions (Time is short; however; we will still get the job done.)

5.6.1 Identify and correctly use prepositional phrases (for school or In the beginning), appositives (We played the Cougars, the team from Newport), main clauses (words that express a complete thought), and subordinate clauses (clauses attached to the main clause in the sentence).

Information Security Questionnaire

Directions: Please answer the questions honestly and to the best of your ability. No one is grading you on your answers, nor is anyone going to know who filled out the questionnaire.

Section 1: Background Information

Age: _____ Racial background: _____

Gender: _____ Grade in school: _____

1. Do you have a computer at home? _____

If you answered no to question one, please move on to question 12.

2. Is your home computer connected to the Internet? _____

If you answered no to question two, please move on to question 12.

3. How are you connected to the Internet at home? (Please choose one)
   a. Dialup service
   b. DSL
   c. Cable
   d. Other _____
4. What Internet service do you use? (AOL, Yahoo, Insight BB, Net Zero, etc.) _____
5. Do your parents use any parental controls with these services to keep you from looking at certain things online? _____
6. About how many hours a week do you think you spend online at home? _____
7. What do you use your computer for at home?

   _____

   _____

   _____
8. What are top the three things that you do most often while online at home? (please circle only 3)

a. Use the Internet for school	b. Talk to friends
c. Email people	d. Play games
e. Download music or programs	f. Look at Websites that interest you
g. Other _____	

9. Would you say that you use your home computer more for school work or more for your own personal use? _____
10. Do your parents have any rules for using the computer? _____

11. If yes, please list some of these rules:

Section 2: True/ False

Directions: Please circle T or F if the answer to the question if it is true or false. If you are not sure about the answer, please circle N.

12. T F N I have used the Internet to download music or programs using file-sharing programs such as Kazaa or Audio Galaxy.

13. T F N I check for viruses when I download a file or open an email attachment.

14. T F N My school uses programs to keep me from looking at Websites that are inappropriate for school.

15. T F N There is nothing wrong with downloading music, videos, or programs for free without permission.

16. T F N When I have an important document for school, I save the file in more than one location, such as on the hard drive and onto a floppy disk or CD.

17. T F N I have been harassed while online by people I did not know.

18. T F N I have been sent inappropriate material while online.

19. T F N *If 17 or 18 were true:* I told my parents or someone in authority when I was harassed or sent inappropriate material while online.

20. T F N I use instant messaging programs such as AOL Instant Messenger, MSN Messenger, Yahoo, ICQ, etc.

21. T F N I use chat rooms.

22. T F N *If 19 or 20 were true:* I chat with people online whom I have never met in person.

23. T F N Sometimes I am not sure if I can trust that the person I am chatting with is who they say they are.

24. T F N I have bought things online.

25. T F N I have bought things online without a parent's permission.

26. T F N I know how to tell if a Website is secure and safe to give information to.

27. T F N A parent or I check for patches or other downloads for my computer to make it safer from hackers.

28. T F N I disconnect from the Internet when I am not using it rather than putting up an away message or simply leaving it connected.

29. T F N I have used or have come in contact with a firewall or filtering software.

30. T F N I use the same password for everything that needs a password.

31. T F N I have used the Internet to make fun of other people or say bad things about them because I knew no one would know it was I who did it.

32. T F N When the allotted trial time has passed on freeware/ shareware, I always either delete the program or purchase it.

33. T F N When the allotted trial time has passed on freeware/ shareware, I have downloaded or borrowed a "crack" for it so I could continue using it for free.

34. T F N I am concerned about someone stealing information about myself when I am online.

35. T F N You can't get in trouble for changing someone's website because it's not "real."

Section 3: Multiple Choice

36. If you see something from a Website that you want to put into a paper you're writing for school, you typically:
    a. Just copy and paste the text into the paper word for word knowing you're never going to get caught.
    b. Copy and paste the text into the paper and then change the words around so it sounds more like something you would write.
    c. Copy and paste the text into the paper and write in the paper where you got the information from.
    d. I've never done any of these before.

37. If you hear a song on the radio that you really like, do you typically:
    a. Go home and download the mp3 from Kazaa or other file sharing service for free.

b. Have your friend download the song and make a CD for you.
c. Go out and buy the CD or have your parents buy it for you.
d. I've never done any of these before.

38. When you receive a file that you are not expecting, you typically:
a. Delete the file immediately without opening it.
b. Open the file to see what it is.
c. Email the sender to find out what the file is.
d. I've never done any of these before.

39. When you receive an email from a person you do not know, you typically:
a. Delete it without opening it.
b. Open it to find out what it is.
c. Email the person back and tell them not to email you again.
d. I've never done any of these before.

40. An example of a good password would be:
a. The name of my favorite character from a TV show
b. My pet's name
c. Taking a line from a song and using the first initial from each word
d. My birthday

41. You are harassed online by someone, you typically:
a. Give it right back. The guy probably deserves it too.
b. Ignore it. Sticks and stones and all that.
c. Report it to the proper authorities or a parent.
d. Block that person's email and screen name.

42. Your teacher leaves a file open on his desktop that contains next week's test and the answer key, and you know he's not going to be back for awhile. Do you:
a. Print out a copy for yourself because he'd never know someone did.
b. Minimize the window so no one else knows that he left it up.
c. Change the questions and answers because he'd never know it was you.
d. Leave it and avoid temptation.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

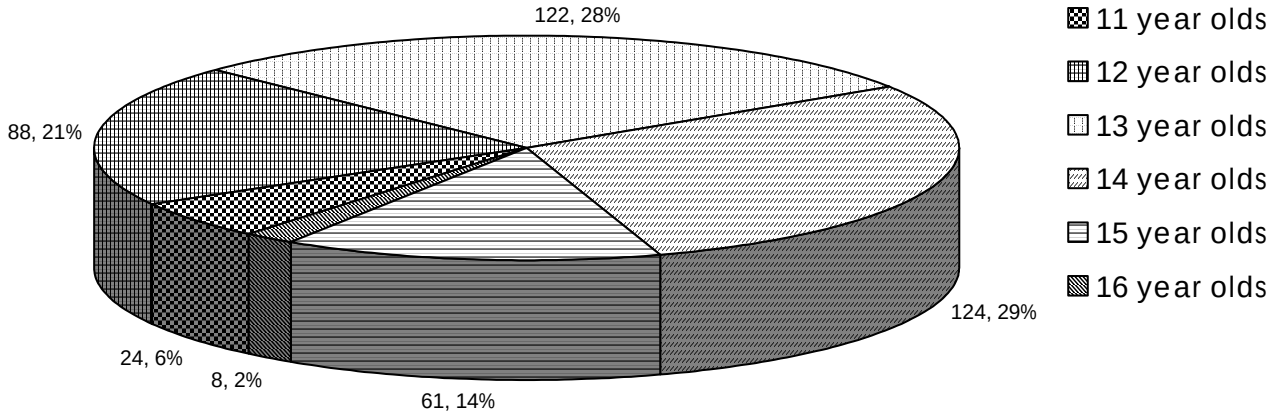
Information Security Questionnaire Results

The following pages contain charts that represent the results of the findings of the Information Security Survey that was given to a total of 488 students from three schools. Sixty-one surveys were thrown out because of inappropriate answers, lack of answers, incorrect age or grade level, etc., leaving a total of 427 valid surveys. Information not included in the compilation is:

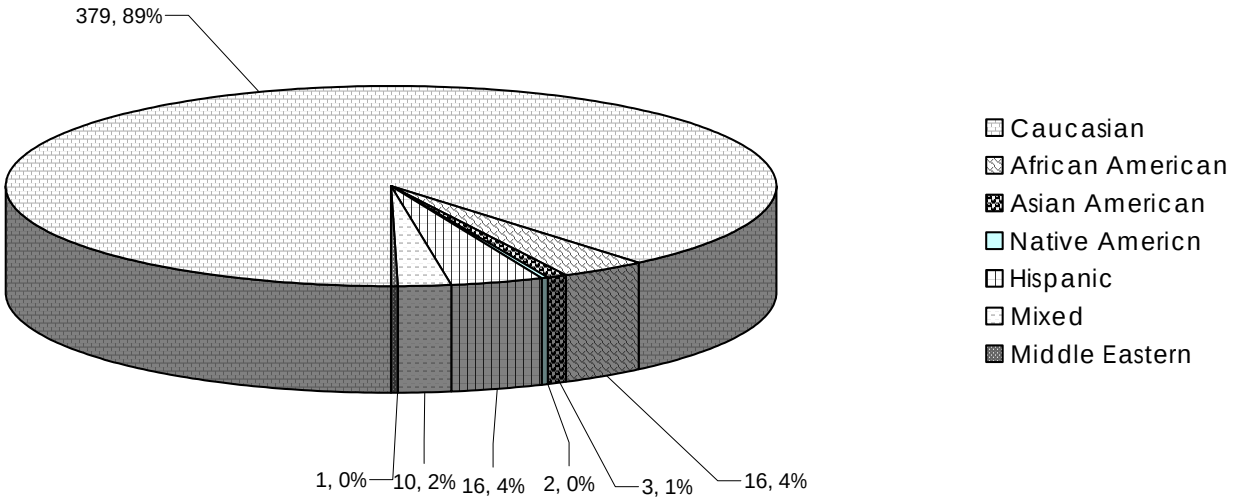
- Gender of those surveyed: There were 214 males and 213 females.
- The chart concerning whether or not the students had a computer was left out because that information could be found on later answers as well, but 408 students did have computers and 19 did not.
- The question concerning which Internet Service Provider. The top five ISPs were:
    - America Online
    - Net Nicto—a local ISP for one of the middle schools
    - MSN
    - Yahoo DSL
    - Insight BB—a local cable company's ISP
- The question concerning specific rules for using the computer was also left out because this was a written answer rather than a more simple answer. The five main rules for using the computer were:
    - Time limits
    - Staying off inappropriate websites
    - Staying away from pornographic websites
    - Asking for permission before using the computer
    - Restrictions on chat rooms or instant messenger

Purdue University ● 656 Oval Drive ● West Lafayette, IN ● 47907-2086
(765) 494-7871 ● Fax (765) 496-3181 ● k-12@cerias.purdue.edu ● www.cerias.purdue.edu

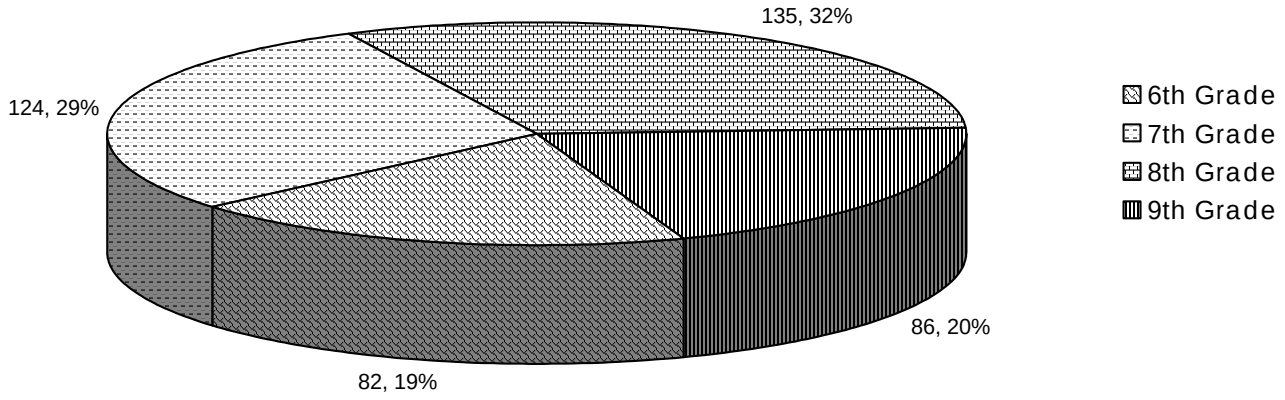
Student Age Distribution



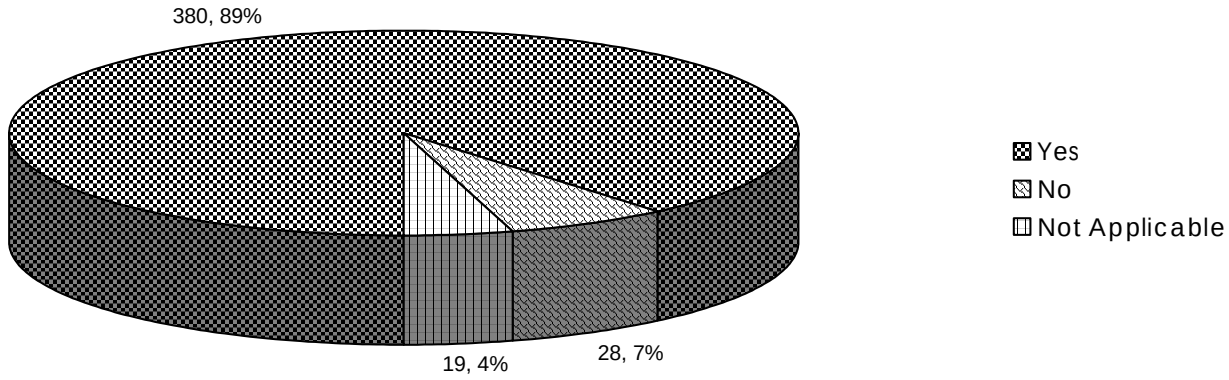
Racial Background



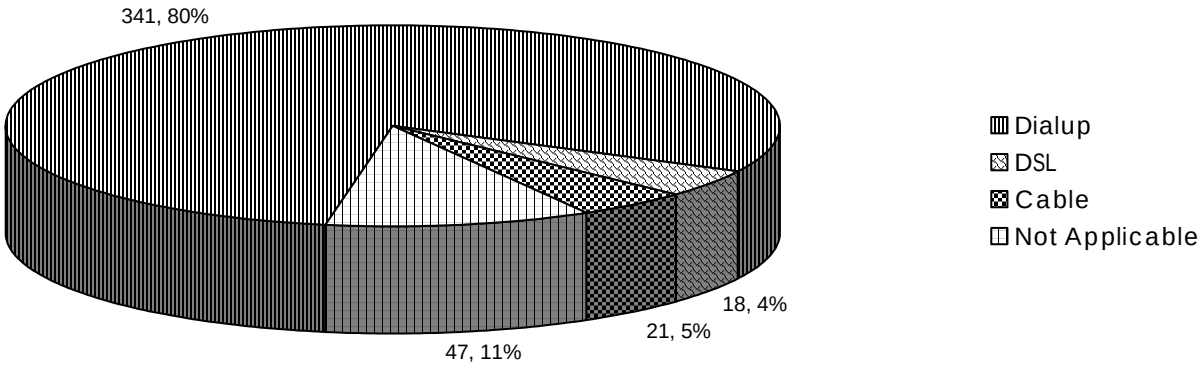
Grade Level Distribution



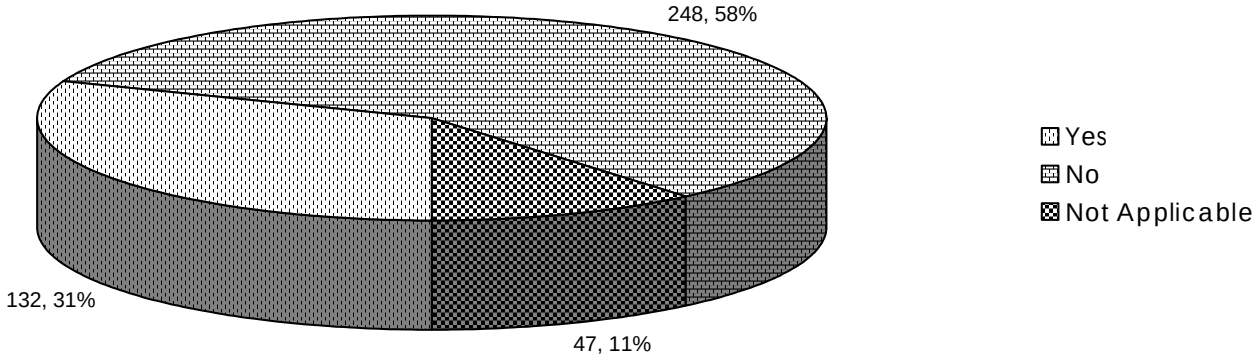
Does Your Home have Internet Access?



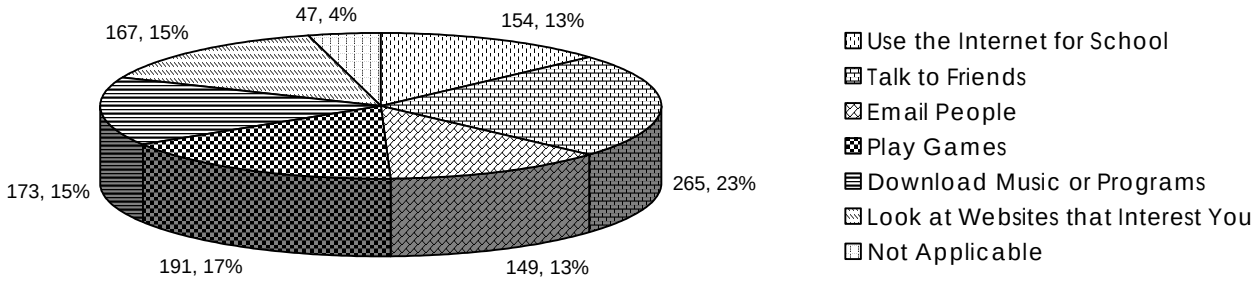
What Type of Connection does your Home Have?



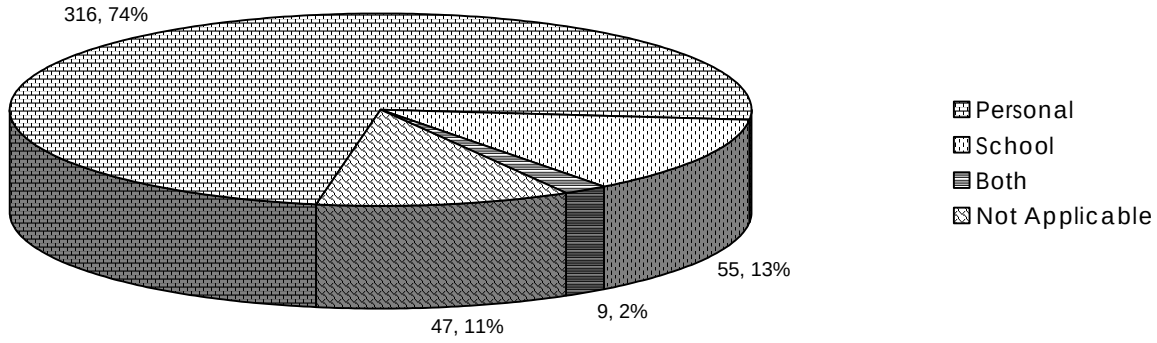
Do Your Parents Use Parental Controls?



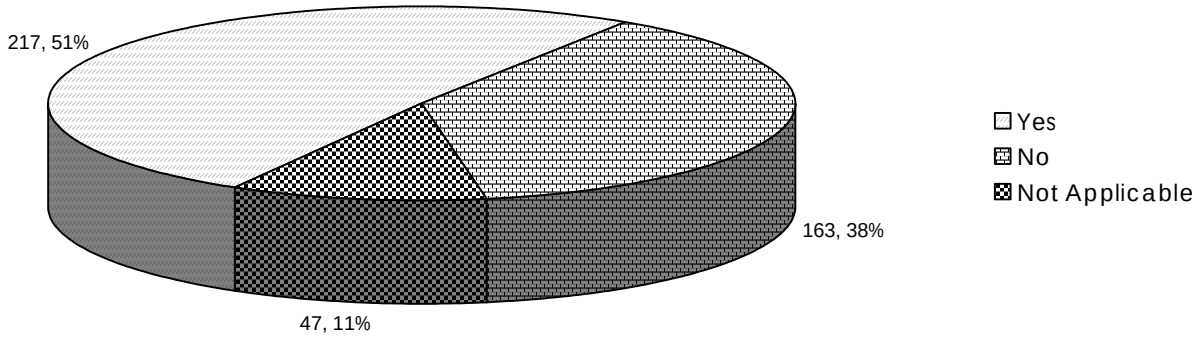
What Are The Top Three Things That You Do Most Often While Online At Home?



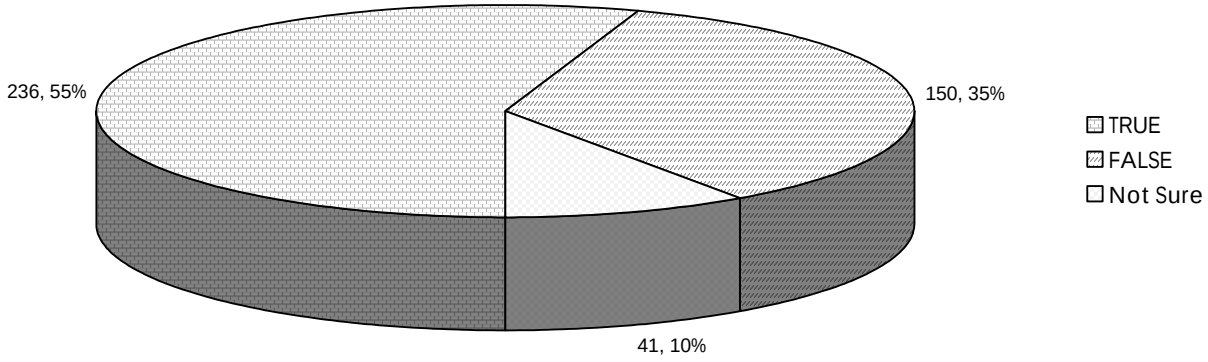
Would You Say You Use Your Home Computer More For School Work Or More For Your Own Personal Use?



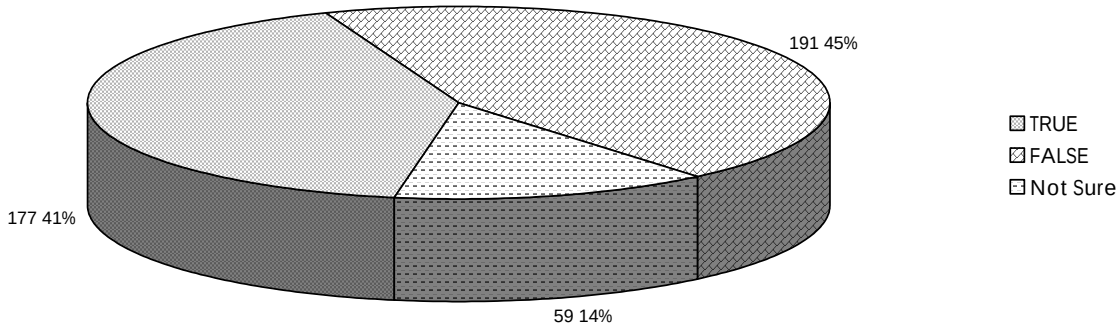
Do Your Parents Have Any Rules For Using The Computer?



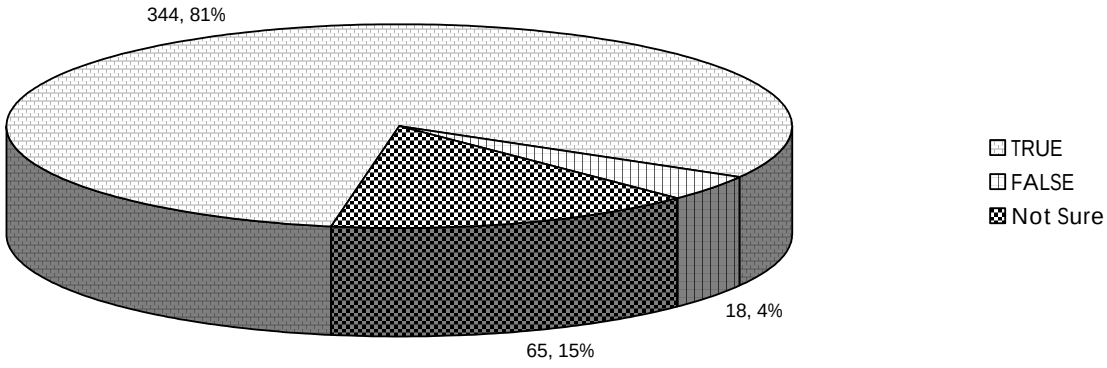
I Have Used The Internet To Download Music Or Programs Using File-Sharing Programs Like Kazaa Or Audio Galaxy



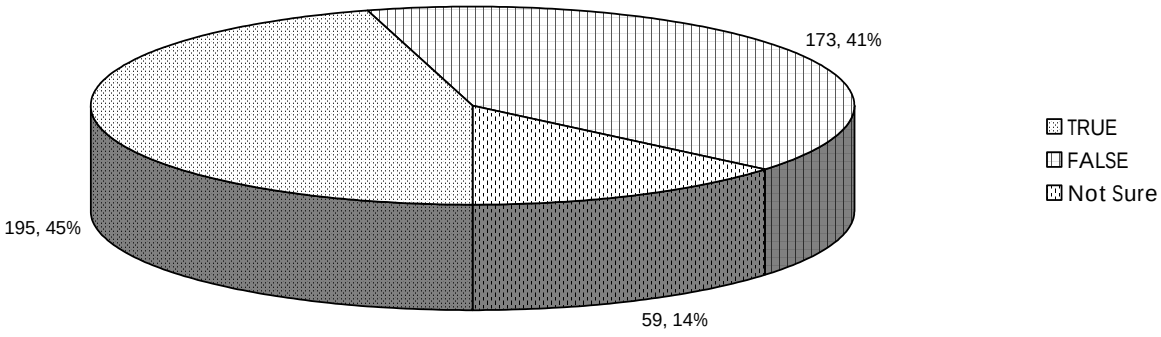
I Check For Viruses When I Download A File Or Open An Email Attachment



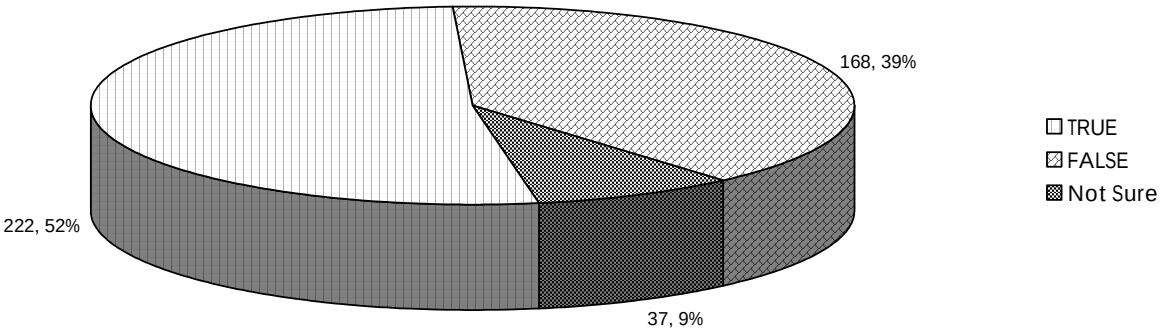
My School Uses Programs To Keep Me From Looking At Sites That Are Inappropriate For School



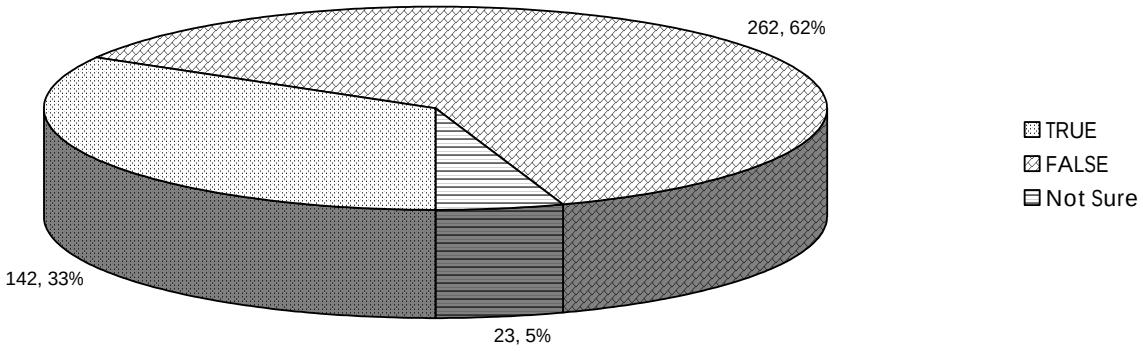
There Is Nothing Wrong With Downloading Music, Videos, Or Programs For Free Without Permission.



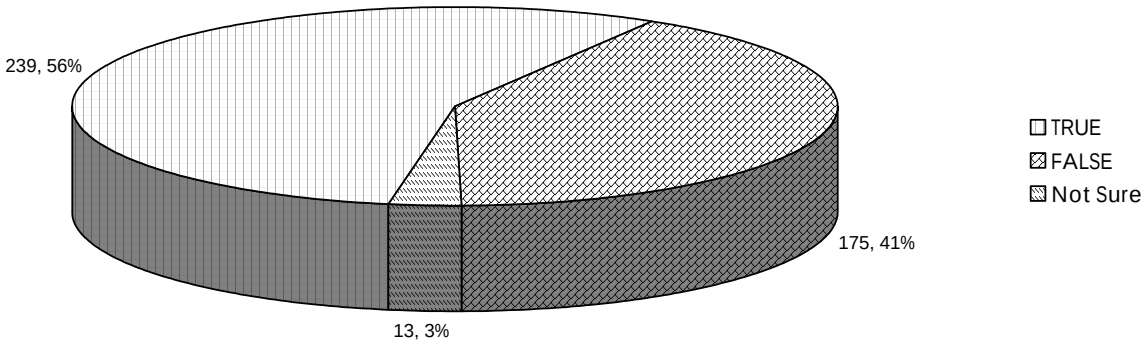
When I Have An Important Document For School, I Save The File In More Than One Location, Such As On The Hard Drive And Onto A Floppy Disk Or CD



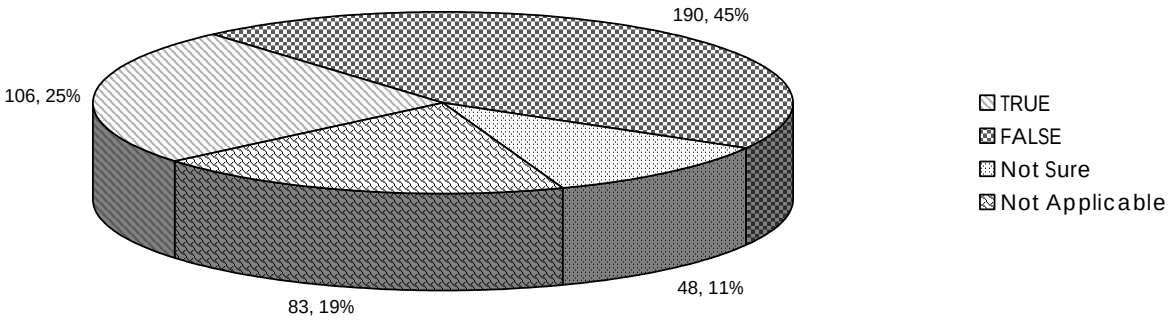
I Have Been Harassed While Online By People I Did Not Know



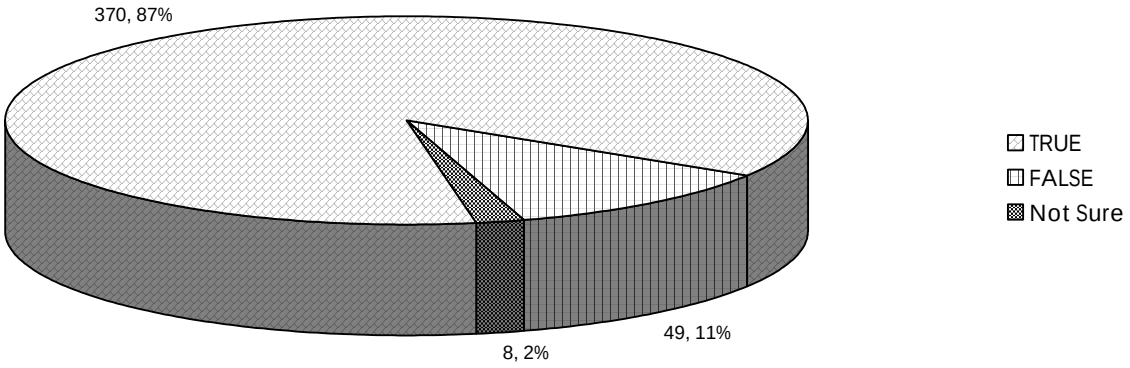
I Have Been Sent Inappropriate Material While Online



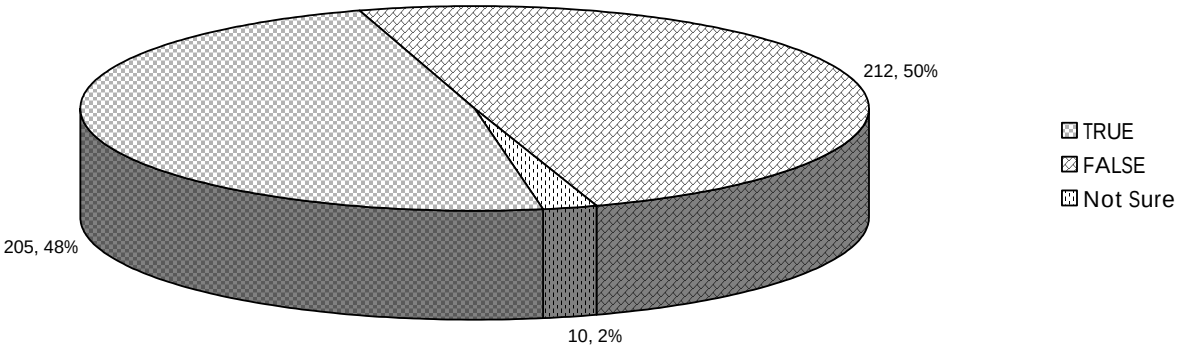
I Told My Parents Or Someone In Authority When I Was Harassed Or Sent Inappropriate Material While Online.



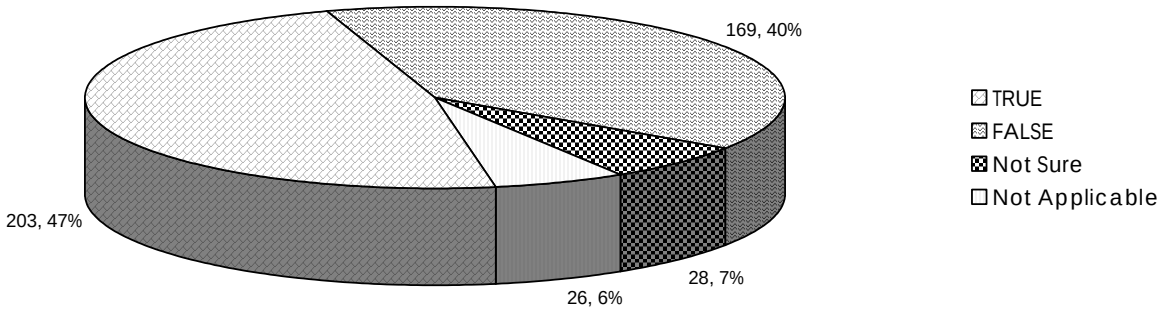
I Use Instant Messaging Programs Such As AOL Instant Messenger, MSN Messenger, Yahoo, ICQ, Etc.



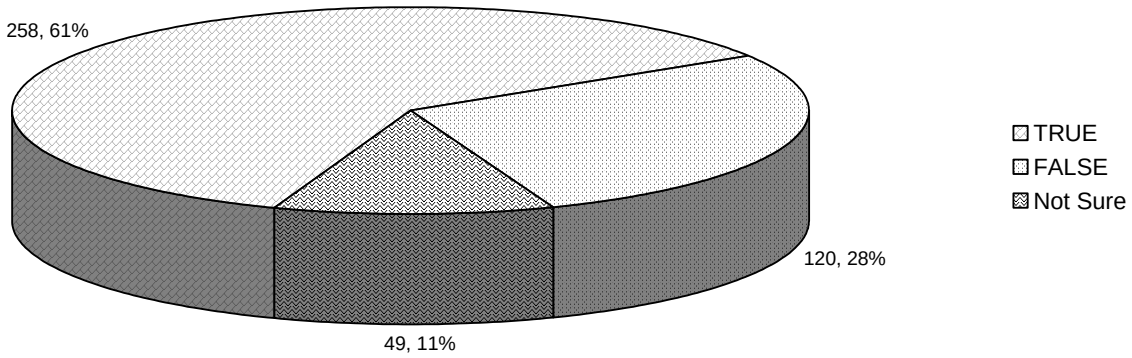
I Use Chat Rooms



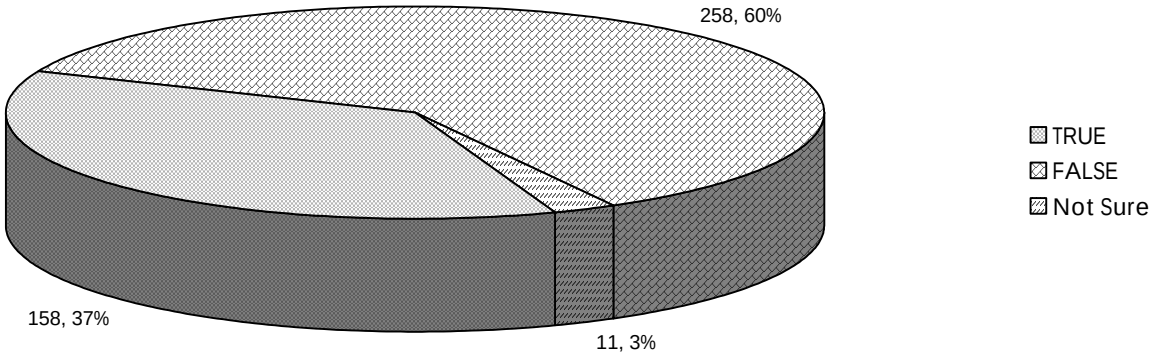
I Chat With People Online Whom I Have Never Met In Person



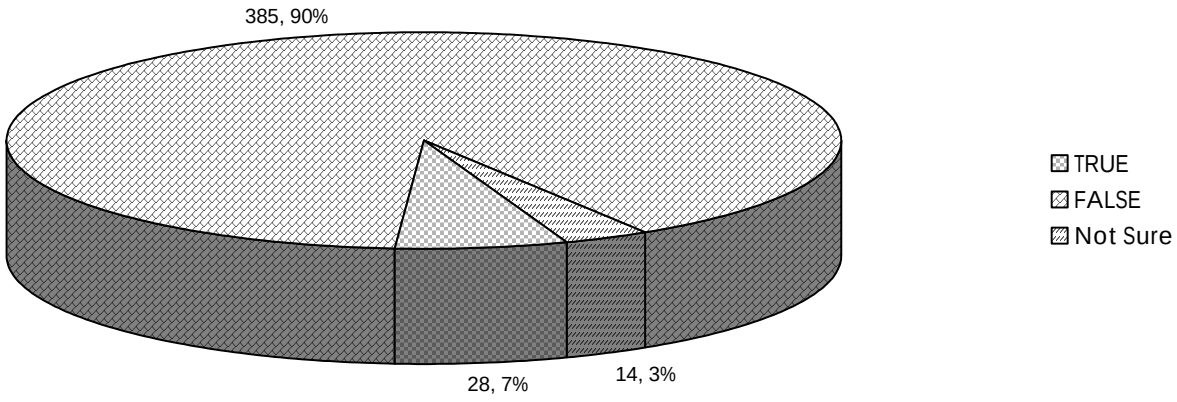
Sometimes I Am Not Sure If I Can Trust That The Person I Am Chatting With Is Who They Say They Are



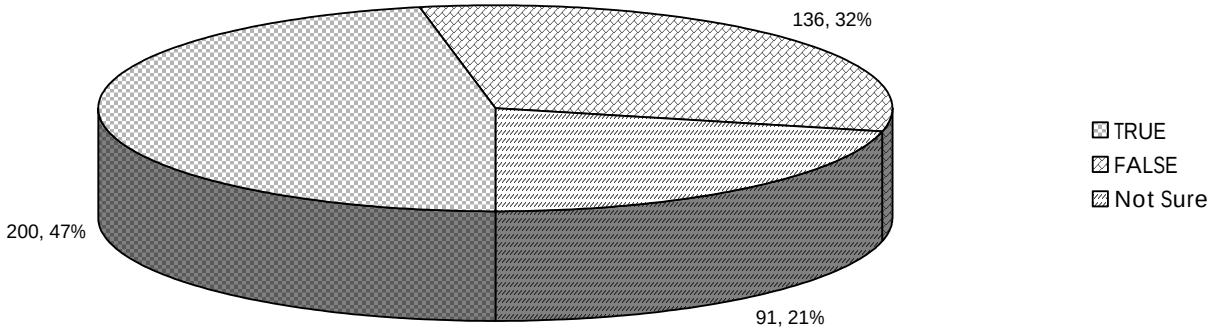
I Have Bought Things Online



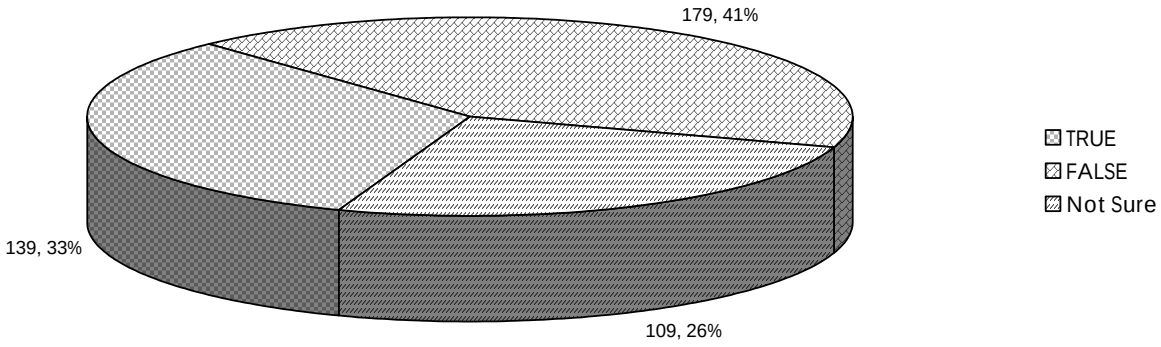
I Have Bought Things Online Without A Parent's Permission



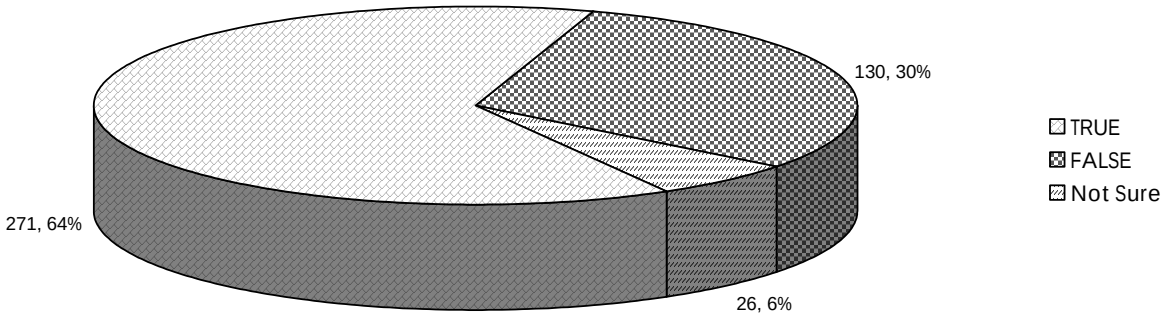
I Know How To Tell If A Website Is Secure And Safe To Give Information To



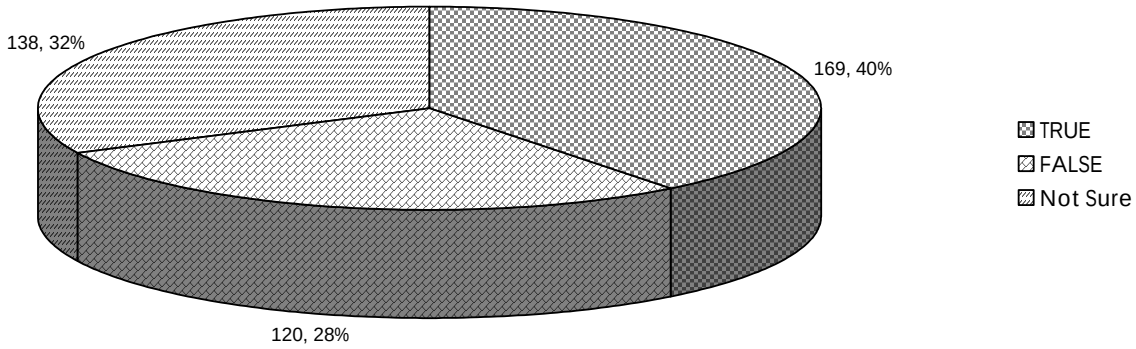
A Parent Or I Check For Patches Or Other Downloads For My Computer To Make It Safer From Hackers



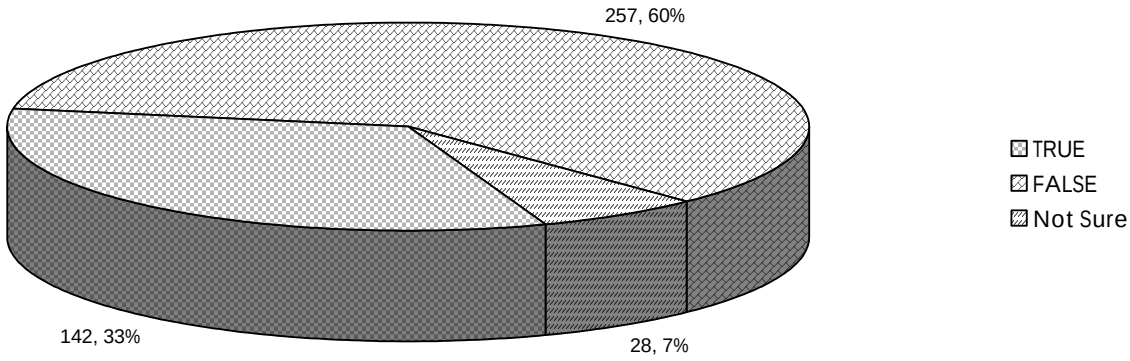
I Disconnect From The Internet When I Am Not Using It Rather Than Putting Up An Away Message Or Simply Leaving It Connected



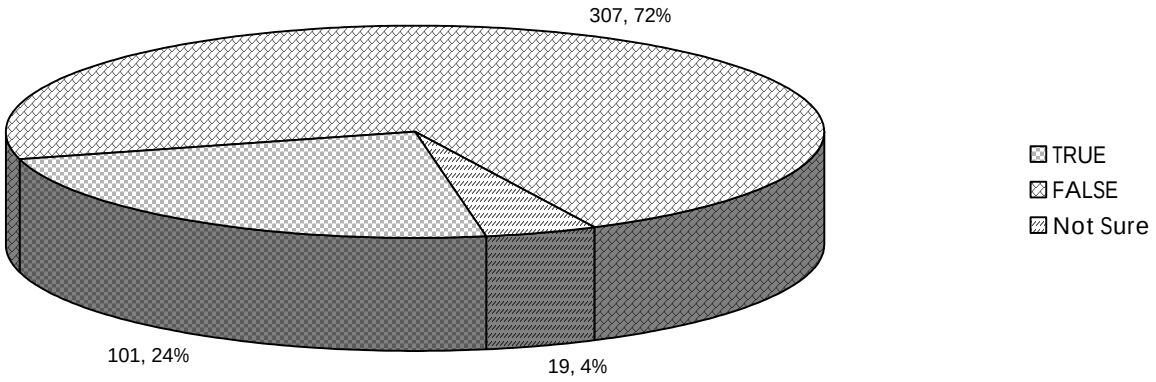
I Have Used Or Have Come In Contact With A Firewall Or Filtering Software



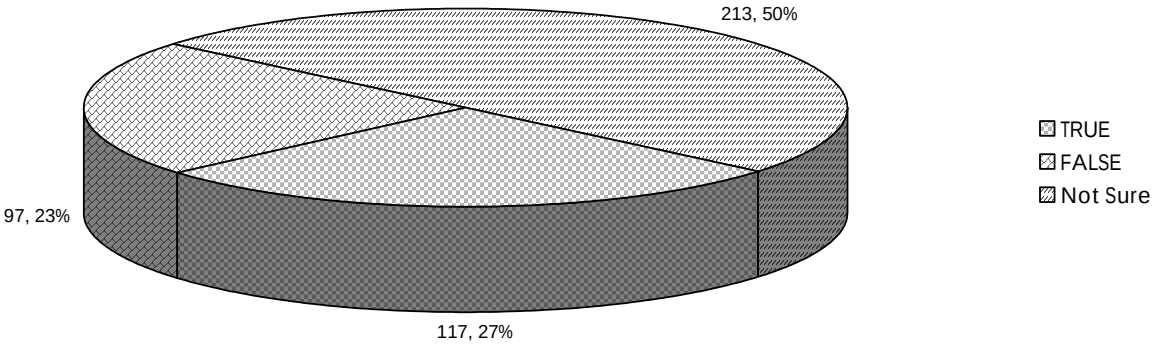
I Use The Same Password For Everything That Needs A Password



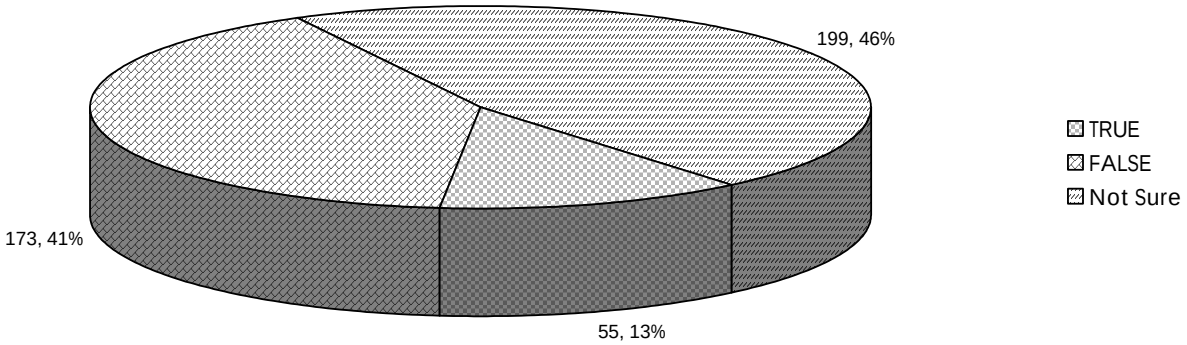
I Have Used The Internet To Make Fun Of Other People Or Say Bad Things About Them Because I Knew No One Would Know It Was I Who Did It



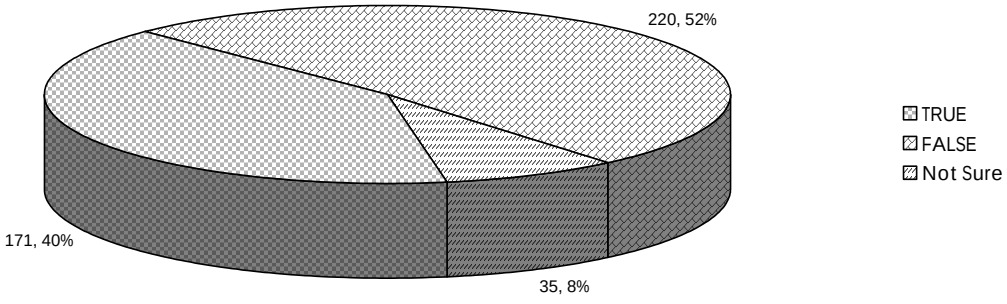
When The Allotted Trial Time Has Passed On Freeware/ Shareware, I Always Either Delete The Program Or Purchase It



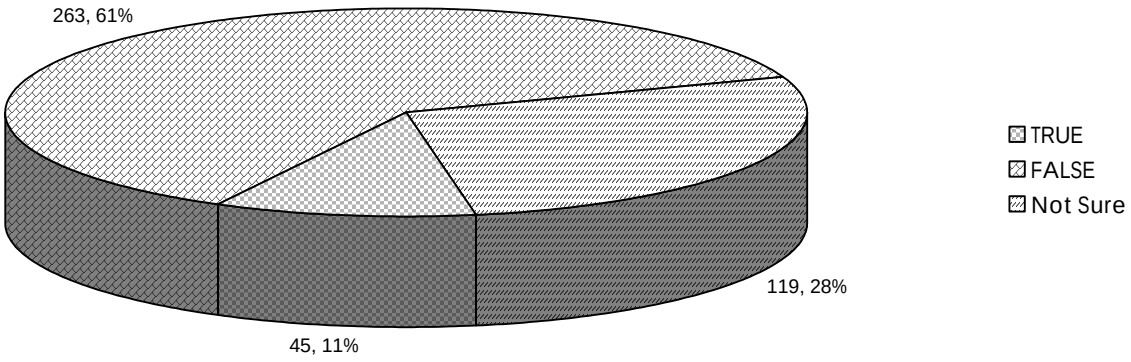
When The Allotted Trial Time Has Passed On Freeware/ Shareware, I Have Downloaded Or Borrowed A "Crack" For It So I Could Continue Using It For Free



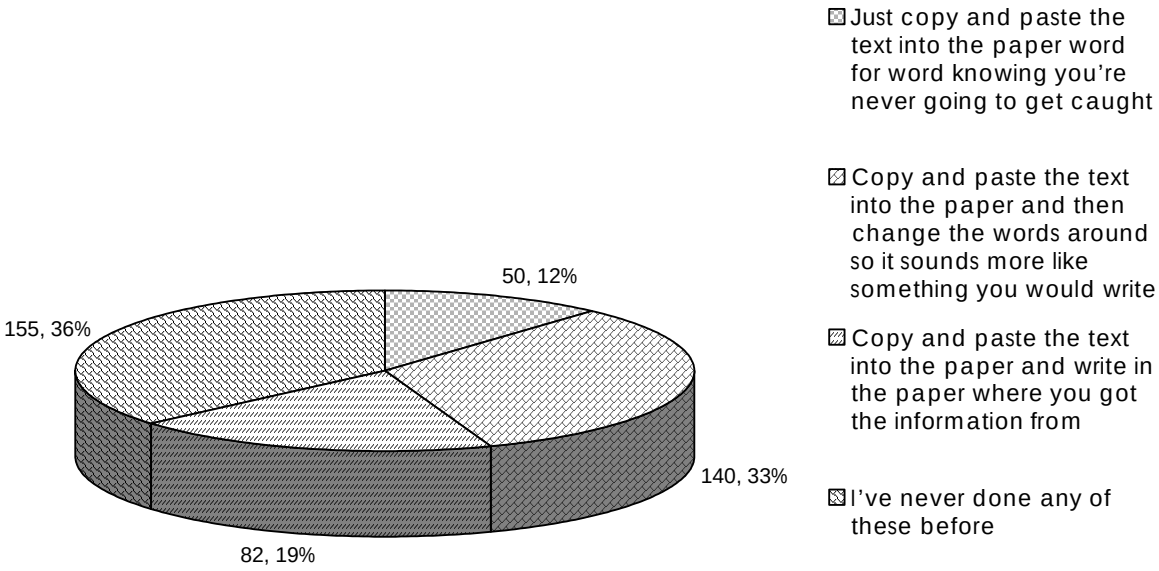
I Am Concerned About Someone Stealing Information About Myself When I Am Online



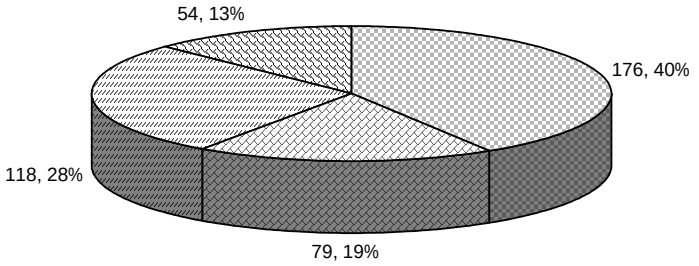
You Can't Get In Trouble For Changing Someone's Website Because It's Not "Real"



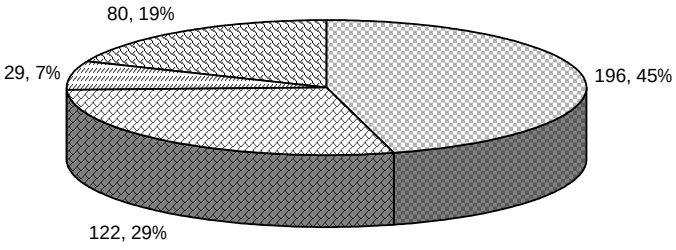
If You See Something From A Website That You Want To Put Into A Paper You're Writing For School, You Typically:



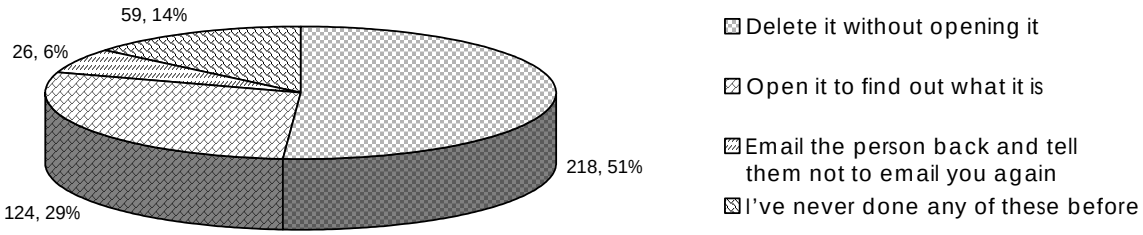
If You Hear A Song On The Radio That You Really Like, You Typically



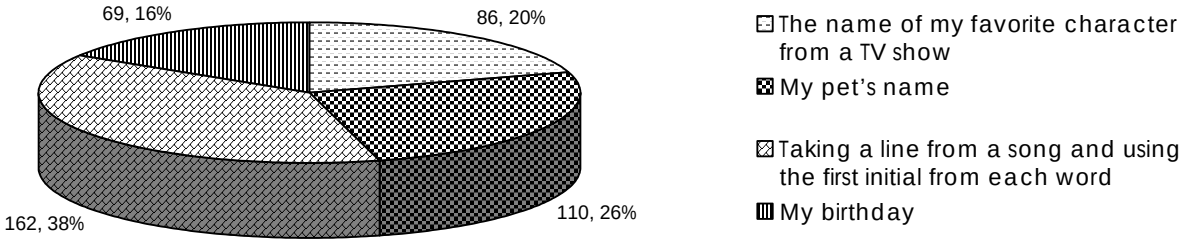
When You Receive A File That You Are Not Expecting, You Typically



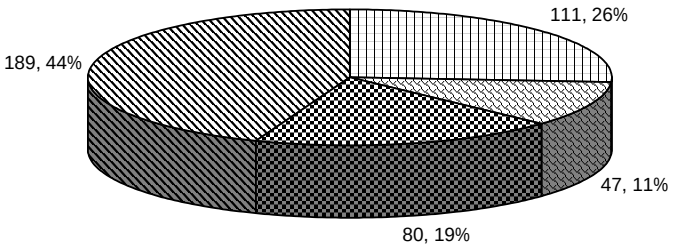
When You Receive An Email From A Person You Do Not Know, You Typically:



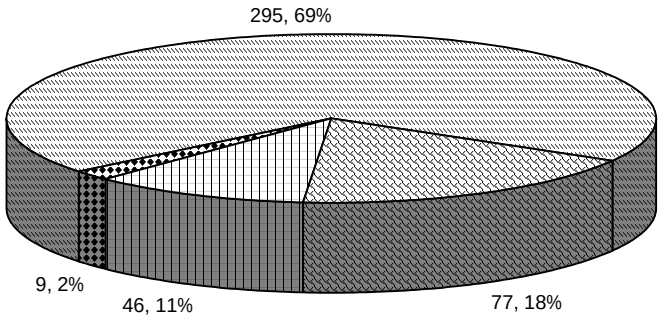
An Example Of A Good Password Would Be



If You Are harassed Online By Someone, You Typically:



Your Teacher Leaves A File Open On His Desktop That Contains Next Week's Test And The Answer Key, And You Know He's Not Going To Be Back For Awhile. You:



Your Guide to Safe Surfing: Learning about the Internet

For Educators:

These materials are the result of a survey given to almost 500 Indiana school children in grades 6-9 in the spring of 2003. The results of that survey showed that middle school students needed more instruction in the basics of how the Internet works, terminology and history, safety concerns, and especially ethical matters.

Your Guide to Safe Surfing: Learning about the Internet is an instructional booklet geared toward middle school students in order to help them learn more about how to use the Internet safely, correctly, and ethically. It is written in the format of a guide for surfing and is themed accordingly. It is divided into three distinct sections: "Treading Water," "Standing up," and "Surfing."

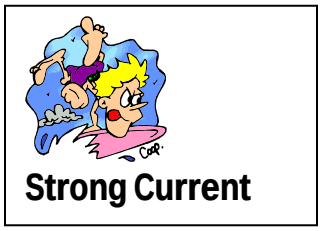
"Treading Water" is separated into three sections: "A Brief History of the Internet," "How the Internet Works," and "Common Terms." "A Brief History of the Internet" is a short timeline that hits the important milestones of the Internet and shows how the system went from a military remnant of the Cold War to the hub of commerce, communication, and information that it is today. "How the Internet Works," much like the previous section, is a short description of how the Internet works in general terms. "Common Terms" is a short glossary of terminology associated with the Internet, with space given for students to add terms as they come across new ones they might need to remember.

"Standing Up" deals with using the equipment properly and effectively and is also divided into three sections: "Using the World Wide Web Effectively," "Using Email," and "Communicating with Others." "Using the World Wide Web Effectively" contains descriptions of the Web, browsers, and URLs. It also contains a Web search exercise dealing with the students' school, finding directions to their homes, and finding websites about their personal interests. "Using Email" looks at how email works and how it's sent and received. Included with this section is an activity dealing with encryption and having students write encrypted messages to their friends and having to decipher them. "Communicating with Others" goes to the next level and looks at chatting and messaging programs and some of the language associated with them, such as emoticons and acronyms/abbreviations. There is an activity associated with this part of the unit where students have to make their own emoticons and abbreviations in relation to their interests and school.

"Surfing" involves the everyday use of the Internet and the issues surrounding that. Like the previous two sections, it is also separated into three parts: "The Ethics of the Internet," "Protecting Yourself from Shark Attacks," and "Knowing the Safe Places to Surf." "The Ethics of the Internet" discusses the student's role in making sure the Internet is free of unethical behavior and how to behave ethically while online. It lists the Ten Commandments of Computer Use (Copyright 1991 Computer Ethics Institute, Author: Dr. Ramon C. Barquin, 1750 K Street, Suite 450, Washington, DC 20006, (202) 296-7147, rbarquin@aol.com) and then has a series of ten short case studies where the students have to identify the unethical action, discuss consequences for the action, who it harms,

and then which commandment it matches and why. "Protecting Yourself from Shark Attacks" shows how people can attack your computer and what you can do to prevent it, and it contains a short exercise matching attacks with their countermeasures. Finally, "The Safe Places to Surf" is a list of safe sites where students can get information and visit without fear of inappropriate material.

Throughout the course of the lessons, there is information off to the sides labeled either "strong current" or "shark warning." "Strong currents" include any secondary information that students might need to know about the subject, typically with Web addresses to sites with extra material, while "shark warnings" deal with the dangers associated with what's being discussed. The booklet is also written in easy-to-understand terms and contains graphics appropriate to the middle school student.



The materials for the students, which are also included in this packet, are written in the **Verdana** font, while the teacher materials are in the Garamond and Century Gothic fonts as seen throughout these pages. Information for teachers will precede the section and the activities, and some parts will be written out so you will be able to make handouts or overheads as you see fit.

The key element of these materials is that they can be used in three different middle school curriculums—English, history/social studies, and science—according to current Indiana state educational standards. The standards with which each activity or set of materials coincide are included in the teacher materials. Suggestions will also be given as to how they can be integrated into your standard curriculum, as well as other activities that could be used with them.

Part I: Treading Water

Goals:

- Students will learn about the history of the Internet through the use of a timeline.
- Students will learn about how the Internet works from a description of how information is sent online from one computer to another via servers.
- Students will learn key terms related to the Internet with the assistance of a glossary.

Description of Sections:

"A Brief History of the Internet"

This first section of "Treading Water" is a timeline showing the history of the Internet from its inception in the early 1960s to what it has become today. Key terms and important contributors to the creation of the Internet as we know it today are listed in **bold** type.

NOTE— The information in the table of contents has two pages—the page it is in the student materials and the page it is in these materials in bold with TM above it rather than SM for student materials.

"Strong Current" Information

Carlson's New Media Timeline—
http://iml.jou.ufl.edu/carlson/professional/new_media/timeline.htm

This website gives a detailed look at the history of the Internet from a more global perspective. The page is split by decade and also split by regions of the world—the UK, the US, Europe, and Asia. It not only looks at the Internet, but also major advancements in technology and multimedia. There are also links within the site that give definitions to some of the more unfamiliar terms.
ARPANET at Webopedia.com—
http://www.webopedia.com/TERM/A/ARPANET.html

This site gives the reader a closer look at the history of ARPANET with links to more information. Links include more information about the birth of the Internet, a more detailed history of ARPANET, and another Internet timeline.

Browser Timelines—
http://www.blooberry.com/indexdot/history/browsers.htm

Provides the user with a history of the four most well-known browsers—Microsoft Internet Explorer, Netscape Navigator, Mosaic, and Opera. Not the most exciting of websites, but it is certainly a good source to find out how Web browsers have evolved over the years.

Suggested Activities with "A Brief History of the Internet"

Have the class break into small groups and give each group a different decade. Have the groups find out what was going on in the world historically as the Internet was evolving and create their own timeline to display in the classroom. Have the students use the Web to find pictures of events and people to put on the timeline as well., then have each group present their information to the class.

"How the Internet Works"

This section describes what it means to be connected to the Internet and how information gets from your computer to someone else's.

"Strong Current" Information

The Animated Internet—http://www.learnthenet.com/english/animate/animate.htm

In less than 50 clicks of your mouse, you can learn how the Internet, the Web, email, mailing lists, search engines, newsgroups, streaming media, encryption, and online shopping actually work. It is explained graphically as well as with text, so it will be easier for more visual learners to understand. Flash is required to view this page, which can be found at www.macromedia.com. While Flash is usually downloaded onto most schools' computers, there is a chance it might not, so always be sure to check the website to make sure it works before you try it in class. If you can't download the program to your school's computers, ask the librarian or an administrator for assistance with getting it installed.

"Common Terms Associated With the Internet"

This is a glossary of words related to the Internet that students might have heard before but not known what they meant. Space is also provided at the end of the glossary so students can write in more words and definitions as they come across them.

Suggested Activities with "Common Terms Associated with the Internet"

- Add a term or two each week to your weekly vocabulary list.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

- Ask students where they have heard these terms before or if they have come across them out in the real world.

State Standards

English

7.2.1 Understand and analyze the differences in structure and purpose between various categories of informational materials.

Science

6.1.9 Explain how technologies can influence all living things.

7.1.5 Identify some important contributions to the advancement of science, mathematics, and technology that have been made by different kinds of people, in different cultures, at different times.

7.1.9 Explain how societies influence what types of technology are developed and used in fields such as agriculture, manufacturing, sanitation, medicine, warfare, transportation, information processing, and communication.

7.1.10 Identify ways that technology has strongly influenced the course of history and continues to do so.

8.1.8 Explain that humans help shape the future by generating knowledge, developing new technologies, and communicating ideas to others.

History:

6.5.5 Identify examples of inventions and technological innovations that have brought about cultural change in Europe and the Americas, and examine their impact.

Your Guide to Safe Surfing: Learning about the Internet

What's inside…

Your Guide to Safe Surfing: Learning about the Internet is designed to help you learn more about what it means to be online today and the dangers and issues associated with being online.

Treading Water, Standing Up, and Surfing

The booklet is split up into three main sections: Treading Water, Standing Up, and Surfing. These sections are divided as follows:

Treading Water

- A Brief History of the Internet
- How the Internet Works
- Common Terms Associated with the Internet

Standing Up

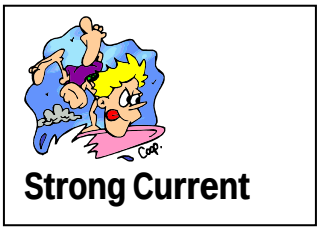
- Using the World Wide Web Effectively
- Using Email
- Communicating with Others

Surfing

- The Ethics of the Internet
- Protecting Yourself from Shark Attacks
- The Safe Places to Surf

Strong Currents and Shark Warnings

Along the way you will see strong currents and shark warnings in the margins. Strong currents lead you to sites on the Internet for further information about a subject, while shark warnings tell you about common dangers associated with the topics being discussed.



Activities

Throughout the booklet you'll find activities and exercises related to the topics being discussed. These are designed to give you hands-on experience with the Internet and ways to associate problems online with problems in the "real world." Space is also provided at the end of this booklet for you to write down any important additional information that you'd like to keep as you learn how to surf the net.

For Further Information

CERIAS, the Center for Education and Research in Information Assurance and Security at Purdue University in West Lafayette, Indiana has further information and activities for you and your parents: http://www.cerias.purdue.edu

Part 1: Treading Water

Although I'm sure most of you have already used the Internet before to play games, talk to friends, or do homework, you might not know why the Internet was created, just how it works, or some of the terms commonly used regarding the Internet itself.

A Brief History of the Internet

Very few people know that the Internet can be traced back as far as the early 1960s! Take a look at the timeline below to find out that it wasn't Bill Gates or Al Gore who invented the Internet, but actually the Department of Defense.

1962 - 1969

The United States Department of Defense's (DOD) Advanced Research Project Agency (ARPA) plans to create a small network of computers called **ARPANET** in order for scientists and researchers to share information.

1969 - 1971

ARPANET connects the first four universities in the United States, the **Stanford Research Institute, UCLA, UC Santa Barbara, and the University of Utah**. By the early 1970s, the ARPANET has become quite popular with many universities, twenty-three total by 1971, with sending email being its favorite use by the researchers.

1972

The InterNetworking Working Group becomes the first organization to keep an eye on ARPANET. **Vinton Cerf** is elected the chairman and later becomes known as a **"Father of the Internet."**

Strong Current

Carlson's New Media Timeline—

http://iml.jou.ufl.edu/carlson/professional/new_media/timeline.htm

A detailed look at the history of the Internet from a more global perspective.

1974

The commercial version of the ARPANET goes online as it becomes less military and more public oriented.

1979

Two grad students at Duke University and a student at the University of North Carolina establish the first **USENET** newsgroups.

1982

TCP/IP, the language of all computers connected to the Internet, is created and becomes the standard language of the Internet by 1983. For the first time the loose collection of networks which made up the ARPANET is seen as an **"internet"**, and the Internet as we know it today is born.

1984

The term **"cyberspace"** is used for the first time in William Gibson's novel *Neuromancer*.

1988

On Nov. 1, 1988, the computer virus was born when a malicious program called the **"Internet Worm"** temporarily disabled 6,000 of the 60,000 Internet hosts. The term "**hacker**" is created. The Computer Emergency Response Team (CERT) is created to address security concerns raised by the Worm.

Shark Warning!

Viruses are still around today, and the only way to prevent them is to have good virus protection software and knowledge on what might be a virus. This will be looked at more in Standing Up.

1990

The ARPANET is shut down for good, leaving the Internet in its place.

1991

The **World Wide Web**, a system of servers that support specific documents, is born. The documents are formatted in a script called **HyperText Markup Language** (HTML), which supports links to other documents, as well as graphics, audio, and video.

The National Science Foundation lifts the restriction on commercial use of the Internet, clearing the way for the age of electronic commerce.

1992

The first audio and video broadcasts take place over a portion of the Internet known as the "MBONE."

Shark Warning!

The World Wide Web and the Internet are NOT the same things! Not all Internet servers are connected to the WWW.

1993

Mosaic, the first graphics-based Web browser, becomes available. America Online releases its PC version.

1994

Marc Andreesen and **Jim Clark** form **Netscape**. Pizza Hut gets an order for a mushroom, pepperoni with extra cheese over the net.

1995

Sun Microsystems releases an Internet programming language called **Java**, and the Yahoo search engine is created.

1996

Approximately 40 million people are connected to the Internet, and more than $1 billion worth of merchandise is bought online.

1999

Shawn Fanning and Sean Parker create the **Napster** peer-to-peer **MP3** file-sharing system, which is used to swap songs for free across the Internet.

Shark Warning!

Although file-sharing programs have been around for some time, it's still illegal and a violation of copyright to download music, video, and programs from programs such as these.

2001

America Online passes the 32 million subscriber mark, adding 1 million in 2-1/2 months. MSN has 7 million and Earthlink has 4.8 million. NetZero counts for 6.1 million users.

Today

Today the Internet is used by tens of millions of people in almost 200 countries across the world. The web is a vast library of information accessible to anyone, anywhere, at any time.

How the Internet Works

Whether you connect from home, school, or outer space, the Internet works the exact same way:

The Internet itself is a global network of separate computers all linked together. It could be looked at as an imaginary space where people can meet up through instant messaging programs or email, or share information or data through their computers and come and go as they please.

The computer uses a modem to connect to an Internet Service Provider (ISP), such as America Online, Microsoft Network, or your local cable company. Sometimes the computers are already connected to an ISP, such as in the case of cable or DSL connections or like your computers at school. At home you sometimes have to call the ISP using a dialup modem.

The ISP's computer is already connected to the Internet, and your computer becomes linked to all the other computers that are connected to that ISP.

Strong Current

The Animated Internet—

http://www.learnthenet.com/english/animate/animate.htm

In less than 50 clicks of your mouse, you can learn how the Internet, the Web, email, mailing lists, search engines, and several other online tools actually work.

Once you're connected, you use a Web browser to navigate the Internet, which communicates with other servers and sends back the information you request when you type an address in the top bar or click on a link to a page.

With the Internet, you have instant access to any piece of information at any time from anywhere. You can communicate with people you would never have had the chance of communicating with before through email or chatting programs. You can listen to music, watch videos, and play games at the click of a mouse. You can go on virtual field trips to other countries or other times in history.

But the Internet is also not without its dangers. Hackers will try everything to get information on your computer, while others will send viruses or talk to you on chat programs to get personal information about you and your family. With the help of this guide, you'll soon learn how to protect yourself from these dangers.

Common Terms Associated With the Internet

Bandwidth—The amount of data that can be passed along a communications channel in a given period of time.

Broadband—Of or relating to or being a communications network in which the bandwidth can be divided and shared by multiple simultaneous signals (as for voice or data or video). It is also faster in speed than dialup. Sometimes referred to as "high speed Internet."

Browser—A program that allows people to navigate specific areas of the Internet.

Cable Modem—High-speed Internet service that is run through your local cable company's lines to your computer.

Database—A computer holding a collection of material arranged for ease and speed of search and retrieval.

Dialup Internet Connection—A network connection which requires that a telephone number be dialed.

Digital Subscriber Lines (DSL)—DSL is a high-speed Internet line that runs through regular phone lines. Also referred to as an "always on" connection because you do not have to disconnect from it in order to use your phone.

Directory—A list of files on an Internet site.

Download—To take a file from another computer and put it on your computer.

Email—A system for sending and receiving messages electronically over a computer network, as between personal computers.

Frequently Asked Questions (FAQ)—A list of frequently asked questions and their answers about a given subject.

File Transfer Protocol (FTP) Site—A publicly-available Internet site where files can be shared.

Gopher—A menu-based system used to find files on the Internet.

Hacker—Someone who uses computers illegally to get information or harm other computers.

Home Page—The opening Web page on an Internet site.

HyperText Markup Language (HTML)—The programming language used to create Web pages.

Hyperlink—A highlighted or underlined word or graphic on a Web page that leads to another Web page.

Internet Account—What allows the user to get online. Typically includes a login, password, and email address.

Internet Service Provider (ISP)—An organization that provides access to the Internet. Some of the better-known ISPs include AOL, MSN, and Yahoo.

Modem—A device that connects the computer to the Internet via phone or cable lines.

Network—A group of connected computers in either a LAN, or Local Area Network, or a WAN, or Wide Area Network.

Search Engine—A Web site that searches the Internet for specific information. This would include engines like Yahoo, Excite, or Google.

Server—A computer that stores information that can be accessed via the Internet.

Other Terms—

Purdue University ● 656 Oval Drive ● West Lafayette, IN ● 47907-2086
(765) 494-7871 ● Fax (765) 496-3181 ● k-12@cerias.purdue.edu ● www.cerias.purdue.edu

Part 2: Standing Up

Goals:

- Students will learn how to use the Web effectively with the assistance of an exercise on using search engines correctly.
- Students will learn about how email works and is sent securely with the use of an exercise on encrypting messages.
- Students will learn about instant messaging and how to chat in that universe with an activity on emoticons and abbreviations.

Description of Sections:

"Using the World Wide Web Effectively"

This first section of "Standing Up" contains descriptions of what the Web is and how it works, the elements of a website, how browsers and search engines work, and it includes any key terms listed in **bold** type. It also contains a Web search exercise dealing with your students' school, finding directions to their homes, and finding websites about their personal interests.

"Strong Current" Information

Dejavu.org, the Web as we remember it—http://www.dejavu.org

This website shows how Web browsers used to work in the "good old days" of the mid 1990s. The emulator includes classic examples of a line-mode browser, Mosaic, Netscape Navigator 1, Lynx, Internet Explorer 1, and HotJava. The site also contains a timeline showing the history of Web browsers.

NOTE— Do NOT type dejavu.COM into your web browser on accident. This leads to a website that has nothing to do with Web browsers.

How Web Pages Work by Marshall Brain—http://computer.howstuffworks.com/web-page.htm

This site gives a more detailed description of how Web pages are programmed, used, and found on the Internet. This site is very technical, going as specific as HTML tagging, but it does include some graphics and good descriptions of what the tags specifically do.

Activity: "Navigating the Web"

"Navigating the Web" is an exercise made for students to learn how search engines use keywords to find the information they are looking for. They first use four search engines in the assignment to find out how many 'hits' they can get about their school, then the students use a search engine to find out information about some of their interests and important sites, then they use it to find out about Boolean phrasing and how they can use it to find information for classes.

Materials

Computers with Internet connections and Web browsers are required for this assignment. If you're going to assign the exercise for homework, make sure all students have Internet capabilities at home or can go to a library or friend's house to work on it.

Procedures

The activity can be done in pairs or alone. If done in pairs, it might be best to pair students so those with more knowledge of the Internet work with those who have less knowledge.

The first part of the assignment asks students to look for information about their school through four different search engines. If your school does not have a Web site, or if your school doesn't have many hits online, have the students look for their favorite college or something associated with what you're currently teaching in class.

The second part has the students find the official sites of the President of the United States, their favorite television show and recording artist, the state's department of education, and the type of computer they're using. With television shows and recording artists, the site is typically the name and then .com at the end, but this is not always true. Having them type the name they're looking for and then "official site" into the search engine usually finds the site they're looking for. If they don't have a favorite TV show or recording artist, change it to sports team, toy, car, movie, etc.

NOTE— Whitehouse.COM is definitely NOT the home page of the President of the United States. Remember that all government organizations end in .gov and NOT .com.

The final part of the activity deals with Boolean phrasing, which is when you use words like 'and' and 'or' or 'not' and quotes in the search boxes to help narrow the search.

Additional Information on Web Page Suffixes

Web pages are created by a variety of organizations, and the type of organization where a page resides often indicates how trustworthy the information on the page will be.

.com – A commercial site. It may be a trustworthy news source that provides current information, or it may be sponsored by a commercial organization attempting to sell you something.

.edu – A site controlled by an educational institution. Usually these sites are carefully monitored and thus trustworthy.

.gov – A government site, often a good source for data or factual information.

.mil – A military site.

.net – A network site, made available to its subscribers with little or no oversight. People who put pages on these sites may or may not be affiliated with an academic or scholarly institution, so be weary of the truthfulness of the information.

.org – The site of a private or non profit organization. Some groups may attempt to influence public opinion, but others are good sources of information.

~ (tilde) followed by a name – A personal home page, published by an individual. Remember, some educational institutions permit individuals to publish home pages with little or no monitoring of the contents, so be careful with these pages as well.

.ca .de .uk .au—These sites are sites from other countries-- .ca is Canada, .de is Germany, .uk is England, and .au is Australia. There are Web pages from countries all over the world, but you'll probably come across these most often. There is a .us, but it's not used unless with international organizations.

Suggested Activities for "Navigating the Web"

Have your students see if they can find themselves online. Have them type their names into a search engine and see what comes up. If they do find themselves online and it's really them and they didn't know that information was online, they could be a victim of invasion of privacy.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

Have students look up information on a subject you're discussing in class using a search engine.

Put a topic into two different search engines to see what sites come up first in the results. Point out to the class that companies pay search engines to come up first in searches, even to come up in the top ten.

State Standards

"Using the World Wide Web," its corresponding activity "Navigating the Web," and any additional suggested activities meet the following state standards:

English

6.2.1 Identify the structural features of popular media (newspapers, magazines, online information) and use the features to obtain information.

6.4.6 Use organizational features of electronic text (on computers), such as bulletin boards, databases, keyword searches, and e-mail addresses, to locate information.

7.2.2 Locate information by using a variety of consumer and public documents.

8.2.1 Compare and contrast the features and elements of consumer materials to gain meaning from documents.

8.4.4 Plan and conduct multiple-step information searches by using computer networks.

Science

6.1.9 Explain how technologies can influence all living things.

7.1.5 Identify some important contributions to the advancement of science, mathematics, and technology that have been made by different kinds of people, in different cultures, at different times.

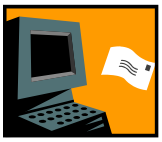
7.1.10 Identify ways that technology has strongly influenced the course of history and continues to do so.

8.1.8 Explain that humans help shape the future by generating knowledge, developing new technologies, and communicating ideas to others.

History

6.5.5 Identify examples of inventions and technological innovations that have brought about cultural change in Europe and the Americas, and examine their impact.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu



"Using Email"

"Using Email" looks at how email works and how it's sent and received. Included with this section is an activity dealing with encryption and having students write encrypted messages to their friends and having to decipher them.

"Strong Current" Information

How Viruses Work by Marshall Brain—http://computer.howstuffworks.com/virus.htm

This site explains how viruses attack your computer and how to prevent them from ever attacking. It is very detailed and very technical, but it does look at how many of the more "famous" viruses worked and how to prevent them today. Be sure to give this site to your students who want to learn everything about the more technical side of the Internet because it has links to just about every element of the net.

Activity: "Encrypting Messages"

"Encrypting Messages" shows students how email messages are put into codes so only people with the correct access can read them. Students are given two blank spaces to write two encrypted messages to a partner with space given at the bottom of the page to decrypt the messages given to them.

Materials

No materials are necessary besides the worksheet. Students might want scrap paper to write their messages on first to make sure they're correct.

Procedures

Break the class up into partners. Read the material as a class and have the partners write an encrypted message to each other. It might be a good idea to write one on your own and put it on an overhead or write it on the board before class starts. If they want to use numbers in their messages, 0-9 would go at the end of the alphabet and then wrap back to A. Have the students tell their partners first if they have numbers in their messages.

Suggested Activities for "Using Email" and "Encrypting Messages"

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

If students don't have an email account, set one up for them on a free email service like hotmail.com. Use the students' email addresses to send messages, assign homework, or use as an advanced organizer.

Encrypt assignments on the board so students will have to decrypt them in order to know what their homework is.

Have students email you written homework assignments as attachments so they can practice sending them.

State Standards

"Using Email," its corresponding activity "Encrypting Messages," and suggested additional activities meet the following state standards:

English

6.2.1 Identify the structural features of popular media (newspapers, magazines, online information) and use the features to obtain information.

6.4.6 Use organizational features of electronic text (on computers), such as bulletin boards, databases, keyword searches, and e-mail addresses, to locate information.

7.2.1 Understand and analyze the differences in structure and purpose between various categories of informational materials (such as textbooks, newspapers, and instructional or technical manuals).

Science

6.1.9 Explain how technologies can influence all living things.

7.1.10 Identify ways that technology has strongly influenced the course of history and continues to do so.

7.1.11 Illustrate how numbers can be represented by using sequences of only two symbols, such as 1 and 0 or on and off, and how that affects the storage of information in our society.

8.1.8 Explain that humans help shape the future by generating knowledge, developing new technologies, and communicating ideas to others.

History

6.5.5 Identify examples of inventions and technological innovations that have brought about cultural change in Europe and the Americas, and examine their impact.

"Communicating with Others"

"Communicating with Others" goes beyond mere mail-based communication and looks at chatting and messaging programs and some of the language associated with them, such as emoticons and acronyms/abbreviations. There is an activity associated with this part of the unit where students have to make their own emoticons and abbreviations in relation to their interests and school.

☺Activity: "Using Emoticons and Abbreviations"

Using emoticons or smileys is a simple way of expressing yourself and adding humor to your emails and IM conversations. These are small graphics created by typing a "face" with text characters sideways. Keeping your email or IMs short and sweet is a good online habit. A good way to do that is by abbreviating phrases or making acronyms of things you'd typically say. This activity helps students make up their own emoticons and abbreviations for things that represent their interests and school.

Materials

No materials are necessary besides the worksheet. Students might want scrap paper to write their emoticons and abbreviations on first to make sure they're correct.

Procedures

Students can work on this assignment alone, in pairs, or in small groups.

Suggested Activities Associated with "Communicating with Others" and "Using Emoticons and Abbreviations"

It is important to stress to the students that Internet shorthand is not the preferred standard of communication when writing papers, business letters, thank you notes to grandma, etc. Keep it in the IM window and not on the research paper.

Have the students speak with the abbreviations they've created:

"IMHO, the movie was so funny that I couldn't help but find myself ROTFL (rolling on the floor laughing). If you see it you'll LOL as well. Well, TTFN."

The difficulty of doing this is a good way to show students that this is really only appropriate for instant messaging and not for the real world.

State Standards

"Communicating with Others," its corresponding activity "Using Emoticons and Abbreviations," and suggested additional activities meet the following state standards:

English

6.2.1 Identify the structural features of popular media (newspapers, magazines, online information) and use the features to obtain information.

7.2.1 Understand and analyze the differences in structure and purpose between various categories of informational materials (such as textbooks, newspapers, and instructional or technical manuals).

Science

6.1.9 Explain how technologies can influence all living things.

8.1.8 Explain that humans help shape the future by generating knowledge, developing new technologies, and communicating ideas to others.

History

6.5.5 Identify examples of inventions and technological innovations that have brought about cultural change in Europe and the Americas, and examine their impact.

Part 2: Standing Up

Using the World Wide Web Effectively

Just what is the Web?

The World Wide Web is the most popular part of the Internet, but it's easy to become overwhelmed by the vast amount of information you can find on it. The Web can be seen as the more exciting part of the Internet due to all the bells and whistles of graphics, animation, sound and video.

So what makes up the Web? The Web consists of your computer, **Web browser** software, a connection to an **Internet service provider (ISP)**, computers called **servers** that host data, and **routers** and **switches** to direct the flow of information. The Web itself is also called a **client-server** system. Your computer is the client; the remote computers that store electronic files are the servers. Here's how it works:

Let's say you want to visit your school's website. First you enter the address or **Uniform Resource Locator (URL)** of the website in your **web browser**, such as Netscape Navigator or Microsoft Internet Explorer. Your browser then requests the web page from the web server that hosts your school's site. The server sends the data over the Internet to your computer. Your web browser reads the data and then displays it on your screen.

Strong Current

Dejavu.org, The Web as we Remember It—

http://www.dejavu.org

A website showing how Web browsers used to work in the "good old days." Also contains a timeline showing the history of Web browsers.

Your school's website also has links to other school websites in your school district. When you click on that link, you access the web server for that school.

The "glue" that holds the Web together is called **hypertext** and **hyperlinks**. This feature allows files on the Web to be linked so you can jump easily between them, and the Web pages themselves are written in a computer language called **Hypertext Markup Language** or **HTML**.

The Elements of a Website

As we just learned, a **website** is a document written in a computer language called **HTML**, short for **Hypertext Markup Language**. Each web page has a unique address, called a **URL** or **Uniform Resource Locator** (1) that identifies what **server** it is connected to on the network.

A website can have one or more web pages depending on how it was made. If there isn't much information, the **home page** (2) may be the only page, but usually you will find at least a few other pages. Much like the table of contents in a book, the home page gives the visitor an overview of what he or she will find on the website. Web pages on a site are linked together by **hyperlinks** (3), which allow you to jump back and forth by clicking on a link.

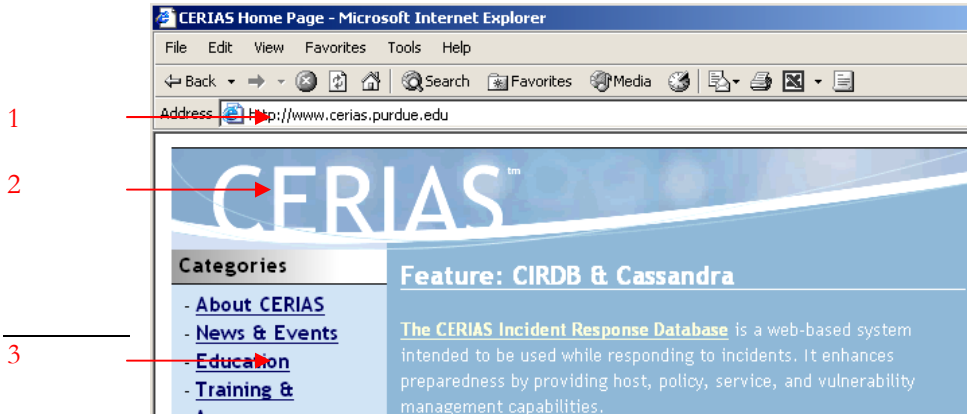
Although websites vary in format and information, they typically follow the same format. At the top of the page is the title of the website, then a list of items, such as other pages, often with a brief description. The items in the list link to other parts of the site or to new sites. These links are highlighted words or images in the body of the text, or they are put in a menu. The text links appear in a different color from the rest of the text and are often underlined. When you move your cursor over a link, it will change from an arrow to a hand, and sometimes words will say what you will link to.

Strong Current

How Web Pages Work by Marshall Brain—

http://computer.howstuffworks.com/web-page.htm

This site gives a more detailed description of how Web pages are programmed, used, and found on the Internet.



Navigating the Web

You will need an Internet-connected computer with a Web browser to complete this activity.

A **Search Engine** is a Web page where you type into a box the **keywords** related to the information that you want. Within seconds the search engine will give you a list of Web sites to try to see if they have the information you're looking for. Not all search engines work in the same way, and you'll often find different pages and totals of pages with each search.

The most Popular Search Engines:

Google http://www.google.com	**Yahoo** http://www.yahoo.com
Alta Vista http://www.altavista.com	**Search.Com** http://www.search.com

Do a search for your school using the four different search engines. List the number of website hits for each search engine. That number appears near the top of the search engine.

Search engine: _____ #of hits _____

Search engine: _____ #of hits _____

Search engine: _____ #of hits _____

Search engine: _____ #of hits _____

With the help of your search engine, find the official sites for the following:

The President of the United States

http://_____

Your favorite television show

http://_____

Your favorite musical group/ artist

http:// _____

Your state's department of education

http:// _____

The computer you're using right now

http:// _____

Use your search engine to look up the definition of Boolean phrasing. Write the definition below:

_____

_____

_____

_____

Give an example of how you would use Boolean phrasing in your own Web searches:

_____

_____

_____

Purdue University ● 656 Oval Drive ● West Lafayette, IN ● 47907-2086
(765) 494-7871 ● Fax (765) 496-3181 ● k-12@cerias.purdue.edu ● www.cerias.purdue.edu

Using Email

As you saw in the timeline, **email** has always been the most popular part of the Internet, and why shouldn't it? It can take days, even weeks to receive a letter in the mail, also referred to as **snail mail; h**owever, you can email someone on the other side of the world in a matter of seconds.

But what exactly is email? In its simplest form, email is an electronic message sent from one computer to another. You can send or receive messages with attachments, such as pictures, school papers, music or even videos.

Follow the Currents

Just as a letter makes stops at different postal hubs along its way, email passes from one computer, known as a **mail server**, to another as it travels over the Internet. Once it gets to where it's going, it's stored in an electronic mailbox until it's opened, and this is all done in a matter of seconds.

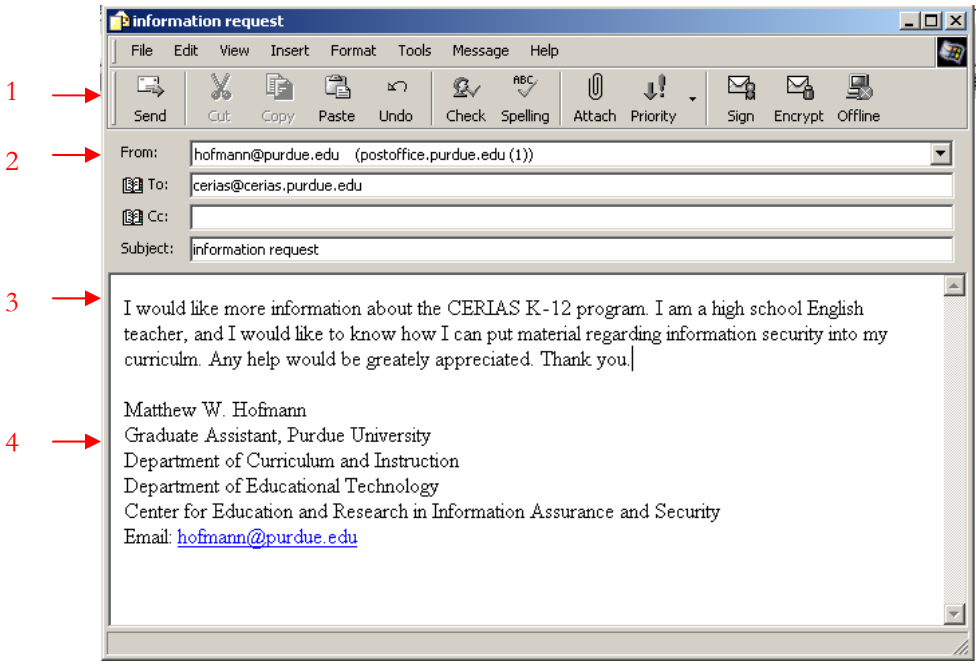
Sending and Receiving Email

To receive email, you must have an account on a mail server, which is like having a home address or PO Box. One advantage email has over regular mail is that you can retrieve your e-mail from any location once you connect to your mail server rather than having to be at home to get letters.

To send email, you need a connection to the Internet through an ISP and access to a mail server. When you send an e-mail message, your computer routes it to a server. The server looks at the e-mail and then forwards it to the recipient's mail server, where it is stored until the recipient retrieves it.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

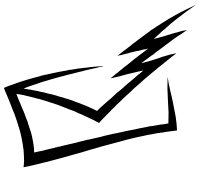
The Anatomy of an Email Message



1. The menu bar. This is where you can send the message, check spelling, attach files, and encrypt the message.
2. This section shows where the message is coming from, who it's going to, where you'd like to send a carbon copy of the message to if you'd like, and the subject line, where you write what the email is about.
3. This is the body of the email. This is where you write your message.
4. This is a signature file. These can be created so you don't have to write the endings of your emails over and over again if you always write them the same way.

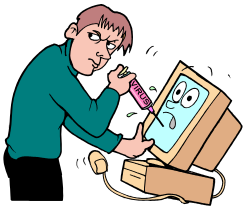
When Sharks Attack Your Email

With email becoming a more common means of communication for everyone, it's important to be aware of all the risks associated with it. Even if you've been using email forever, you might not always be aware of ways that it can be used to attack your computer.



Email spoofing is a common attack that occurs when an email message looks like it's come from one person, usually someone you know, when it actually was sent from another source. Spoofing is often an attempt to trick you into sending information like passwords. It can range from harmless pranks like email chain letters to social engineering ploys. One example of social engineering includes email that appears to have

come from a system administrator requesting users to change their passwords to something suggested by the sender. Another example would be an email claiming to be from a person in authority requesting users to send them a copy of a file or other information. Remember that while ISPs like America Online may occasionally request that you change your password, they usually will **not** specify what you should change it to. Also, most ISPs would **never** ask you to send any password information or file via email. If you think that you may have received a spoofed email from someone, you should contact your service provider's support personnel immediately.



Viruses and other types of malicious code are often spread as attachments to email messages. Before opening any attachments, be sure you know where the attachment came from and what type of file it is. Many email viruses are known to use hidden file extensions. The files attached to these messages may appear to be harmless text, MPEG, AVI or other file types, but the file is actually malicious script or executable virus programs—.vbs, .exe, or .bat files, for example. Always read the entire file name before opening attachments.

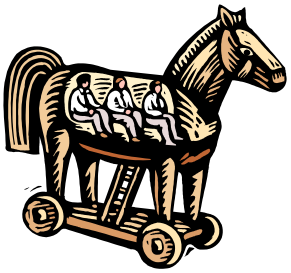
Strong Current

How Viruses Work by Marshall Brain—

http://computer.howstuffworks.com/virus.htm

This site explains how viruses attack your computer and how to prevent them from ever attacking.

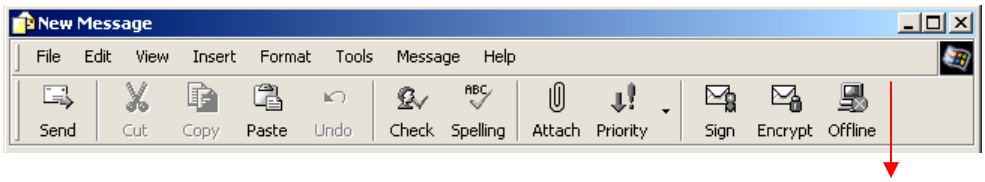
Trojan horse programs are a common way for hackers to trick you into installing "back door" programs, which can allow them easy access to your computer without you knowing. They can reprogram your OS or infect your computer with a virus. Hackers will also frequently use these infected computers as launching pads for attacking other computers by installing an "agent" that runs on the infected computer and waits for further instructions. Then, when a number of agents are running on different computers, a single "handler" can instruct all of them to launch an attack on another system, making the end target of the attack not your computer but someone else's -- your computer is just a convenient tool in a larger attack.



The safest thing to do when you receive an attachment or file from someone that you're not expecting is to email that person back and ask him if he sent you a file. If he didn't, then delete it. If you receive an attachment from someone you don't recognize at all, don't even think twice. Delete the file immediately.

Encrypting Messages

One of the ways to make sure no one can read your email is using what's known as **encryption**. Encrypting a message means to change a file or message using a secret code so people that you don't want to read it can't. When you send an email to someone, you can encrypt the message by clicking on the encrypt button at the top of the menu bar:



Once you click on the encrypt button, the mail program will turn the message into a secret code when you send it, and only the person receiving the email will be able to read it.

Although this sounds like new technology, encryption has been used for centuries, as early as ancient Rome. Julius Caesar would code his messages by using character shifting. The message is encrypted by shifting forward each character of the alphabet a fixed number of characters.

For example, shifting by 1 changes **a** to **b**, **b** to **c**, and so on. Letters at the end the alphabet are encrypted by starting at the beginning. In other words, **z** becomes **a**. If it shifts by 3, **a** becomes **d, b** becomes **e**, etc. Going backwards with the procedure is called **decryption.**

Activity:

Encrypt a message to a partner. Be sure to put the number you wish them to encrypt by or they won't be able to figure out what you wrote!

Now try it with a different number:

Communicating With Others

The Miracle of Instant Messaging

Instant Messaging (IM) has exploded in popularity. It's more immediate than e-mail and cheaper than a phone call. Almost one billion instant messages are sent across the Net each day using the four most popular IM services: AOL Instant Messenger, ICQ, MSN Messenger and Yahoo Messenger, and they all work in the same way.

After signing up for the service by creating a user name and password, you build what is known as a "buddy list," which contains the people that you want to talk to online. When any of the contacts on your list are online, you can initiate a private chat with that person.

So how does the IM software know who's online? When you start the program, it connects with the service's IM server and logs you on. The server then checks your buddy list to see if any of your contacts are also logged on, and your list updates to show you who is currently online. At the same time, your contacts' lists update to indicate that you're online as well. By clicking on a name you can send text messages to that person. After you type your message and hit return, the message travels to the IM server, then immediately forwards to your buddy's computer.

Shark Warning!

Members of one instant messaging service can't communicate with those using another. If most of your buddies use the same service, however, it's not a problem. There's also nothing to stop you from using more than one service, but it does make things a little more complicated at times.

Shark Warning!

Instant messages can not be encrypted, so conversations can be watched by attackers. This means that any information you wouldn't want strangers to know should never be talked about on IM programs.

☺ Using Emoticons and Abbreviations

Using emoticons or smileys is a simple way of expressing yourself and adding humor to your emails and IM conversations. These are small graphics created by typing a sideways "face" with text characters. Here's a short list of examples:

:-) Basic smiley	8-) Nerdy smiley	5:-) Elvis smiley
;-) Winking smiley	O:-) Angel smiley	:-X Not talking
:-(Sad smiley	:-* Kissing smiley	(-: Left handed
:-D Laughing smiley	:-& Tongue tied	:-> Sarcastic

Come up with five smileys of your own that you might use to represent your heroes or your school or your interests and put them in the blanks below and write what they are:

_____--_____

_____--_____

_____--_____

_____--_____

_____--_____

Keeping your email or IMs short and sweet is a good online habit. A good way to do that is by abbreviating phrases or making acronyms of things you'd typically say. Here are a few examples:

TTFN—Ta Ta For Now	LOL—Laugh Out Loud
BF—Boyfriend	OIC—Oh I See
IMHO—In My Humble Opinion	BRB—Be Right Back

Come up with five abbreviations of your own that you might use to represent things you normally say or your school or your interests and put them in the blanks below and write what they mean:

_____--_____

_____--_____

_____--_____

_____--_____

_____--_____

Strong Current

Using abbreviations or acronyms is also a good way to make passwords. Instead of using your pet's name or your birthday, take a line from a song and take the first letter from each word and use that for your password instead. Use a zero instead of the letter O or a one instead of an I to make it harder to figure out!

Used with Permission

PURDUE
UNIVERSITY

The Center for Education and Research in Information Assurance and Security

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

Part 3: Surfing

Goals:

- Students will learn about the ethics of the Internet with the assistance of mini case studies.
- Students will learn about the four common attacks to computers and the three common countermeasures to them with the assistance of a matching exercise.

Description of Sections:

"The Ethics of the Internet"

"The Ethics of the Internet" discusses the student's role in making sure the Internet is free of unethical behavior and how to behave ethically. It lists the Ten Commandments of Computer Use (Copyright 1991 Computer Ethics Institute, Author: Dr. Ramon C. Barquin, 1750 K Street, Suite 450, Washington, DC 20006, (202) 296-7147, rbarquin@aol.com) and then has a series of ten short case studies where the students have to identify the unethical action, discuss consequences for the action, who it harms, and then which commandment it matches and why. **NOTE:** There is a copy of the Ten Commandments of Computer Use at the end of this section that is appropriate to make into copies or an overhead for use with the activities.

Activities: Mini Case Studies

This is a series of ten short, one-paragraph case studies dealing with different elements of cyber ethics. Questions look at what the unethical action is, who's at fault, which of the Ten Commandments of Computer Use the actions match up with, possible punishments for the unethical action, real world examples of the action, who the action affects, etc.

Materials

No materials are required besides the activity sheets and a writing utensil.

Procedures

The activities can be done alone, in pairs, in small groups, or as a class. It might be a good idea to do the first one or two as a class so students can hear different opinions about what others believe to be the unethical action or appropriate punishments for the actions.

"Strong Current" Information

"Ethics in the Age of Digital Photography" by John Long—
http://www.nppa.org/services/bizpract/eadp/eadp.html

This site looks at the issue of photo manipulation and the ethical issues surrounding it. It has several more examples of how the media uses photo manipulation in order to make images more exciting, cleaner, or just able to fit on the page. This is an excellent source to discuss how ethical issues affect us every day and debate when photo manipulation is ethical and not.

Safekids.Com—
http://www.safekids.com

Produced by the Online Safety Project, Safekids.com has a discussion of safety issues, including privacy issues. It contains guidelines and tools for parents on how to make online activities safer for their families, a quiz that tests students' online safety knowledge, and links to sites with additional information.

The Software & Industry Information Association Anti-Piracy Page—
http://www.spa.org/piracy/default.asp

This is an excellent source for finding out about anti-piracy laws and reporting software theft. It includes a FAQ for answering your questions about anti-piracy issues and also lists locations for further information about piracy and its prevention.

The Purdue University Online Writing Lab—http://owl.english.purdue.edu

The OWL is the single greatest source online for learning how to cite sources for papers. It contains information on MLA and APA documentation, tips for dealing with plagiarism, writing resumes and cover letters, and just about anything else associated with writing.

"The Napster Cantata" by M.A. Kabay—
http://networking.earthweb.com/netsysm/article.php/625221

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

A point-by-point discussion about downloading music and responses to all the excuses you use for downloading music. This is a great source to fight the student who seems to have all the answers about why it's alright to download music.

"Purdue Cracks Down on Downloading" by Jenny Jones—
http://www.purdueexponent.org/interface/bebop/showstory.php?date=2003/02/24&section=campus&storyid=illegaldownloads

An article concerning how Purdue University is dealing with the music downloading issue and the steps they take to discipline the students who do. This shows students that there are actions taken against those who do illegally pirate music from the Internet.

Association of Shareware Professionals—
http://www.asp-shareware.org/

This website has an excellent FAQ to answer all your questions about shareware.

Suggested Activities Associated with "The Ethics of the Internet" and the mini case studies

Introduce the section at the beginning of the school year in your class and do activities throughout the year as the assignments seem fitting. For example, use "A Rose by the Same Name" when talking about writing research papers so students know what plagiarism is and how to site sources correctly. Use "Kiera's Downloading Dilemma" when talking about current events or controversial topics. Use the mini case studies in association with debates or discussions about the positives and negatives of technology in society.

State Standards

"The Ethics of the Internet," its corresponding mini case study activities, and suggested additional activities meet the following state standards:

English

6.2.8 Note instances of persuasion, propaganda, and faulty reasoning in text.

6.7.9 Identify persuasive and propaganda techniques used in electronic media (television, radio, online sources) and identify false and misleading information.

7.2.1 Understand and analyze the differences in structure and purpose between various categories of informational materials (such as textbooks, newspapers, and instructional or technical manuals).

7.2.3 Analyze text that uses the cause-and-effect organizational pattern.

7.4.5 Identify topics; ask and evaluate questions; and develop ideas leading to inquiry, investigation, and research.

7.4.6 Give credit for both quoted and paraphrased information in a bibliography by using a consistent format for citations.

8.2.2 Analyze text that uses proposition (statement of argument) and support patterns.

Science

6.1.9 Explain how technologies can influence all living things.

7.1.5 Identify some important contributions to the advancement of science, mathematics, and technology that have been made by different kinds of people, in different cultures, at different times.

7.1.9 Explain how societies influence what types of technology are developed and used in fields such as agriculture, manufacturing, sanitation, medicine, warfare, transportation, information processing, and communication.

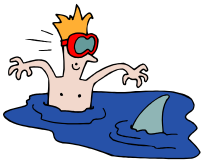
7.1.10 Identify ways that technology has strongly influenced the course of history and continues to do so.

8.1.7 Explain why technology issues are rarely simple and one-sided because contending groups may have different values and priorities.

8.1.8 Explain that humans help shape the future by generating knowledge, developing new technologies, and communicating ideas to others.

History

6.5.5 Identify examples of inventions and technological innovations that have brought about cultural change in Europe and the Americas, and examine their impact.
8.2.3 Identify and explain the relationship between rights and responsibilities of citizenship in the United States.
8.2.4 Define and explain the importance of individual and civic responsibilities.
8.2.13 Research and defend positions on issues in which fundamental values and principles related to the Constitution of the United States are in conflict, using a variety of information resources.



"Protecting Yourself from Shark Attacks"

"Protecting Yourself from Shark Attacks" shows how people can attack your computer and what you can do to prevent it, and the section contains a short exercise matching attacks with their countermeasures.

"Strong Current" Information

How Firewalls Work by Jeff Tyson—http://computer.howstuffworks.com/firewall.htm.

This site explains what firewalls are and how they block attacks to your computer. Like the other "how stuff works" sites, this one is also very technical and not for the casual passerby.

Activity: "Attacks and Countermeasures"

"Attacks and Countermeasures" takes the information learned from "Protecting Yourself from Shark Attacks" and puts it into a matching exercise where the students must think critically in order to match the attack with what type of attack it is and the countermeasure needed to combat it.

Materials

The only materials needed are the information before the activity, the activity itself, and a writing utensil.

Procedures

Activity can be done alone, in pairs, small groups, or as a class. After reading the directions, it might be a good idea to do the first one as a class. Several of them have more than one possible solution, so stress that to the class as well.

Answers

Attack	Type of Attack	Countermeasure
Little brother keeps accidentally using sister's account	Human unintentional	**Policy**—rules and consequences for using others' accounts **Procedural**—password-protected accounts
Power surge	Environmental manmade	**Technical**—surge protector
Someone asks you for your password	Human intentional	**Policy**—never give your password to anyone

Extreme summer heat	Environmental natural	**Technical**—air conditioner **Policy**—don't use computer outside if a laptop or shut off during the day
Inappropriate email	Human intentional	**Policy**—never open email from people you don't know
Hackers	Human intentional	**Technical**--firewall
Mom keeps erasing disks without checking them	Human unintentional	**Policy**—making it a rule to always check disks before erasing them with appropriate punishment for doing so
You're sent a file that attacks Windows	Human intentional	**Technical**—purchase anti-virus program **Procedural**—set up the program **Policy**—set up rules and consequences for not checking files
Your sister keeps leaving the computer connected to the net	Human unintentional	**Policy**—make rules and consequences for staying connected to the Internet when not at the computer
You forget to run the anti-virus program	Human unintentional	**Procedural**—have anti-virus program auto-run at set times

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

Suggested Activities Associated with "Protecting Yourself from Shark Attacks" and "Attacks and Countermeasures"

Have the students go home and see what kinds of attacks they're vulnerable to at home. Have them come up with what kinds of attacks they are and the countermeasures needed to control them.

State Standards

"Protecting Yourself from Shark Attacks," its corresponding activity "Attacks and Countermeasures," and any additional activities meet the following state standards:

English

7.2.3 Analyze text that uses the cause-and-effect organizational pattern.

Science

6.1.9 Explain how technologies can influence all living things.

History

6.5.5 Identify examples of inventions and technological innovations that have brought about cultural change in Europe and the Americas, and examine their impact.

"The Safe Places to Surf"

"The Safe Places to Surf" is a list of Websites that are appropriate and safe to use by middle school students. A more thorough list of Websites can be found online at http://www.cerias.purdue.edu/k-12/. Be sure to look at the full list yourself to see if there are sites there that you can integrate into your curriculum as well.

Part 3: Surfing

The Ethics of the Internet

When you do anything online, whether it's sending email, buying things, talking on instant messenger, or simply looking at websites, you can sometimes feel like nothing can stop you from doing anything to anyone else, whether it's wrong or not. Just as much as there are rules for saying and doing certain things in the real world, there are rules for conducting yourself properly on the Internet. The problem with this is that even though you're taught in school and at home how to say please and thank you and that words hurt just as much as actions, you're not taught the ethics of the Internet. However, as the Internet becomes more and more an element necessary for survival, it is more important than ever to think about the concept of ethics and apply it to the Internet.

The idea of cyber ethics, or the responsibility of appropriate Internet behavior, is a rather new one. Think of it in terms of what you choose to do online when no one else is looking. If you do the same things online by yourself as you would if a parent or teacher were sitting right next to you, you probably have very good cyber ethics. If you're constantly minimizing windows or quickly shutting down programs as your mom or dad enter the room, your cyber ethics might need to be worked on a little.

The Computer Ethics Institute has defined The Ten Commandments for Computer Ethics (Copyright 1991 Computer Ethics Institute, Author: Dr. Ramon C. Barquin, 1750 K Street, Suite 450, Washington, DC 20006, (202) 296-7147, rbarquin@aol.com), and they are:

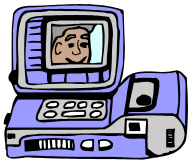
1. **Thou shalt not use a computer to harm other people.**
   - This would include not just hacking into another computer, but also using websites or email to send out hateful information about someone else, a school, or place of business.
2. **Thou shalt not interfere with other people's computer work.**
   - This would be any sort of interruption in someone's normal routine online or at his computer. Although you'd probably like to put pop-up ads in this category, you really can't.
3. **Thou shalt not snoop around in other people's files.**
   - Any time you look at someone else's files without probable cause, you're in violation of their right to privacy.
4. **Thou shalt not use a computer to steal.**
   - Never take anything off someone's computer without permission.
5. **Thou shalt not use a computer to bear false witness.**
   - Don't use your computer in order to lie about other people or events.
6. **Thou shalt not use or copy software for which you have not paid.**

- You are permitted to make one copy of a program for personal use, as long as neither the original nor the copy will be used at the same time.

7. **Thou shalt not use other people's computer resources without authorization.**
   - Just as you should ask first before you use someone else's things in the real world, you should ask before you use someone else's space on their computer, web page, or email.
8. **Thou shalt not appropriate other people's intellectual output.**
   - You cannot steal anyone else's copyrighted material regardless of whether or not you think it's right, what you want to steal is too expensive, or if you don't think you could possibly ever get caught.
9. **Thou shalt think about the social consequences of the program you write.**
   - Anything that anyone could potentially see needs to be looked at in terms of whether or not it could hurt others emotionally or threaten someone in some way. Laws in cyberspace apply just as much as they do in the real world, and harassment is harassment anywhere.
10. **Thou shalt use a computer in ways that show consideration and respect.**
    - You should always use your computer in a way that is never harmful to anyone else, whether it's by word or deed.

The following is a series of ten situations dealing with different ethical problems related to the Internet. Read each of the short situations and answer the questions after them. You will have to refer back to the Ten Commandments of Computer Ethics for these exercises as well.

Peter's Digital Camera Hijinks



The Situation:

Peter has been using his parents' digital camera to take pictures for his family's Web page. While cropping and resizing pictures, Peter has found that he can use the same program to change certain elements of his pictures. He has since made himself look thinner, his dad bald, and has also removed his little sister completely from all pictures. Peter has since put these pictures up on the family's website.

Questions:

1. What is the unethical action? Who is at fault?

2. What discomfort might Peter cause? To whom?

3. What sort of punishment should Peter be given for this action?

4. Are there real world incidents that are similar to this?

5. Which of the 10 Commandments of Computer Ethics does this relate to and why?

Examples of Photo Manipulation:

Many people think that photo manipulation only occurs when kids have too much free time and a really good computer, but it happens in all sorts of places.

The first set of photos comes from an issue of *Time* magazine during the OJ Simpson trial. The picture on the right is the actual police photo, while the one on the left is what was run on the cover of *Time*. Notice how the photo was manipulated so Simpson was given more of an unshaven look and the background made darker to give him a more sinister, guilty look. Also notice how his number was made smaller so the bottom line could be put into frame.

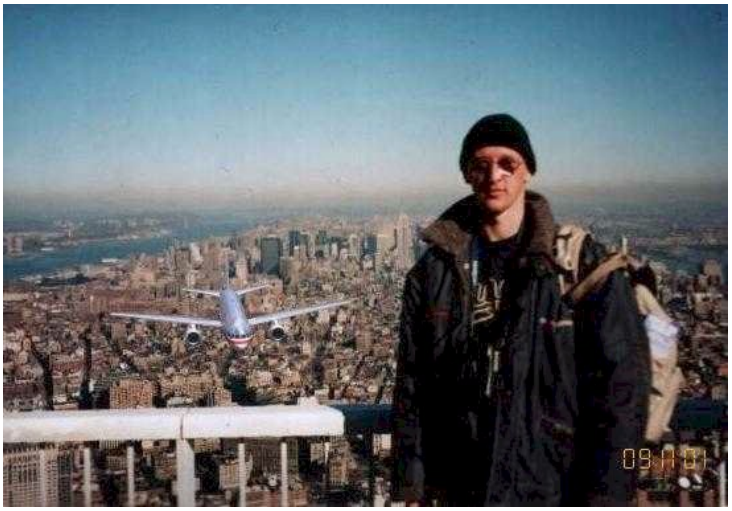
The following photo was digitally altered as well. It was made to look like the person in the photo and the other person taking the photo were on top of one of the World Trade Center towers right before one of the planes hit it on September 11, 2001. It was later discovered that the photo was taken by a Hungarian man in 1997 at the World Trade Center and that the plane, which is actually the wrong plane and coming from the wrong direction, was added by using Photoshop.

Strong Current

"Ethics in the Age of Digital Photography" by John Long—

http://www.nppa.org/services/bizpract/eadp/eadp.html

This site looks at the issue of photo manipulation and the ethical issues surrounding it. It has several more examples of how the media uses photo manipulation in order to make images more exciting, cleaner, or just able to fit on the page.



If you still don't believe that the picture could possibly be fake, perhaps instead of a plane New York could be attacked by aliens on a hazy day:

Or perhaps the man in the hat could be on the Moon:

Closing:

While Peter's actions might seem like good, clean fun, integrity is a serious issue which even young people need to be aware of. Deliberate tampering of events may harm both those involved in the event as well as the reputation of the one who tampered. The purpose of a family Web site is to have a lasting record of the activities and appearance of individuals, not to be a place to make fun of your own family.

Just because magazines and news organizations change photos doesn't mean it's right. Take steps now to be honest and true to your work, and you know that you'll be doing the right thing in the future.

James and the Giant Joke Site

The Situation:

James has found a Web site containing jokes about African Americans, Hispanics, and women. He prints the pages out and shares them with his friends and also sends several jokes to people via email.

Questions:

1. What is the unethical action? Who committed it?

2. What discomfort might James's action cause?

3. What would be an appropriate punishment for such an action?

4. Can you think of real world incidents that would be similar to this?

5. Which of the 10 Commandments of Computer Ethics does this relate to and why?

Closing:

Not all "bad stuff" on the Internet is pornography, but a good deal of it is certainly offensive and not all that educational. It's important to realize when something becomes inappropriate for use. If you think that something you found on the Internet could be offensive to anyone, don't share it.

Anthony's Internet Survey

The Situation:

Anthony fills out a survey on a gaming page. The survey asks for his email address, his home address, and a list of what types of games he plays. He readily fills in this informaiton. In the following weeks, he receives junk mail at home as well as dozens of emails about new games.

Questions:

1. Whose privacy is at risk? What discomfort has filling out the survey caused?

2. Do you fill out surveys like this while online? Why or why not?

3. What are the advantages and disadvantages of a business knowing your personal likes and dislikes?

4. Is there a parallel in the real world to this situation?

5. Which of the 10 Commandments of Computer Ethics does this relate to and why?

Closing:

Businesses and organizations use personal information to market products. Sometimes this information is collected without your permission or awareness that it is being collected at all. An organization that is given information may even sell it to other organizations.

Shark Warning!

Web sites use what are called "cookies" to track where you're going online. This is another way for the people online to get more information about you and your interests. These can be blocked by changing the settings of your Web browser.

When Carrie Met Mark

The Situation:

Carrie "meets" Mark, who shares her interest in cars, in an Internet chat room. After several conversations over following weeks, Mark asks Carrie for her home telephone number and address.

Questions:

1. Whose privacy is at risk?

2. What danger might Carrie get in if she gives Mark her information?

3. Is there a safe plan of action Carrie might take to meet Mark?

4. Is there a parallel in the real world to this situation?

5. Which of the 10 Commandments of Computer Ethics does this relate to and why?

Closing:

A stranger is a stranger, whether you meet them in the school parking lot or in a chat room. The same rules about real world strangers apply to online strangers as well. The fact that we cannot get clues about a person from his or her physical appearance (age, race, gender) adds to the difficulty in judging whether that person is safe.

Strong Current

Safekids.Com—

http://www.safekids.com

Produced by the Online Safety Project, Safekids.com has a discussion of safety issues, including privacy issues.

Kenny's Email Usage

The Situation:

The principal believes that Kenny has been using his school email account to send threatening and inappropriate messages to other students in the school. He asks the school's technical coordinator to give him copies of all of Kenny's emails.

Questions:

1. Whose privacy is at risk? Why?

2. What ethical and legal issues are related to the principal reading Kenny's emails?

3. What responsibilities do parents and schools have in making you aware of how much privacy you have?

4. Is there a real world example you can relate this to?

5. Which of the 10 Commandments of Computer Ethics does this relate to and why?

Strong Current

Your school should have an acceptable use policy regarding how you can use your school's computers. If you have never seen it, ask your teacher or school librarian for a copy.

Closing:

It is still debatable whether schools have the right to search files that are created and stored on an organization's computer hardware like they do lockers or book bags. You're on their property and using their property. Students are more than aware that weapons can be stored in backpacks and lockers, and for the safety of all children in a school officials sometimes need to invade a student's privacy when there is a good reason. Could computer files and emails ever be so dangerous that safety concerns should override privacy concerns?

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

George's Wandering Eyes

The Situation:

George's teacher leaves her computer to go to the office. While she is gone, George finds she has been working on a test for the class that he's in, and her word processing program is still open. He decides to see what the questions are.

Questions:

1. Whose privacy is at risk? How?

_____

_____

2. What danger or discomfort might the unethical action cause?

_____

_____

3. What could George's teacher have done differently to keep George from looking at the test?

_____

_____

4. Are there incidents in the real world similar to this situation?

_____

_____

5. Which of the 10 Commandments of Computer Ethics does this relate to and why?

_____

_____

Closing:

Just because information accidentally left out does not mean that it is alright to access it. Is forgetting to lock the front door the same as allowing someone to enter it? It's no different than getting in trouble for looking at someone's diary or reading over someone's shoulder. It's an invasion of privacy.

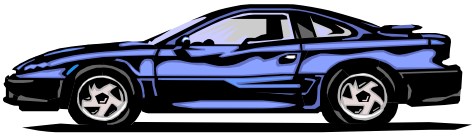
Strong Current

Intellectual Freedom Committee of the American Library Association—

http://www.ala.org/alaorg/oif/privacygandа.html

This site answers all your questions about privacy and confidentiality in reference to being online.

Grand Theft Video



The Situation:

Peter borrows Anthony's copy of *Grand Theft Auto* and installs it on his computer. He tells Anthony that he will either uninstall the game if he doesn't like it or buy his own copy if he does.

Questions:

1. What is the property? Who is its owner?

2. What danger might keeping the game on Peter's computer cause?

3. Is digital media more likely to be illegally copied than more tangible media like books or videos? Why?

4. Is there a situation in the real world similar to this scenario?

5. Which of the 10 Commandments of Computer Ethics does this relate to and why?

Closing:

It is unethical and illegal to make copies of programs without the permission of or payment to the creators of those programs under copyright law. When you buy a game, you're really only purchasing the right to use it. The ownership of the

Strong Current

The Software & Industry Information Association Anti-Piracy Page—

http://www.spa.org/piracy/default.asp

An excellent source for finding out about anti-piracy laws and reporting software theft.

game code itself still stays with the creator of the program, which means that someone cannot change the program or resell it. The general rule is that one copy of a program be purchased for each computer on which it is to be run. And no, being unable to pay for software is not a good excuse for illegally copying any more than the inability to pay for a CD is any justification for shoplifting it from a music store.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

A Rose by the Same Name

The Situation:

Rose finds information about *Romeo and Juliet* for her Shakespeare project on a CD encyclopedia in the library. She uses the copy function to take an entire paragraph from the entry and then pastes it into her paper word for word. She also doesn't write down the title of the entry or the CD encyclopedia. When she writes her report, Rose doesn't cite the source in her works cited page.

Questions:

1. What is the property? Who is its owner?

2. What harm might this action cause?

3. Do you think the plagiarism is on purpose or due to a lack of understanding? Why? Does it matter?

4. What real world incidents are similar to this situation?

5. Which of the 10 Commandments of Computer Ethics does this relate to and why?

Strong Current

The Purdue University Online Writing Lab—

http://owl.english.purdue.edu

The OWL is perhaps the single greatest source online for learning how to cite sources for papers.

Closing:

It is important to learn how to cite sources in both print and electronic formats. Although plagiarism is sometimes done on purpose, much of it comes from a lack of understanding as to what and when to cite as well. Whenever the information in a paper isn't from your own head, you must cite the source.

Kiera's Downloading Dilemma

The Situation:

Kiera hears a song on the radio that she really likes. She goes home and downloads the song from a file-sharing program. While using the program Kiera thinks of several other songs she likes, downloads them, and burns her own mix CD of her favorite songs.

Strong Current

"The Napster Cantata" by M.A. Kabay—

http://networking.earthweb.com/netsysm/article.php/625221

A point-by-point discussion about downloading music and responses to all the excuses you use for downloading music.

Questions:

1. What is the property? Who is its owner?

2. What danger does Kiera's unethical action cause?

3. Is downloading music from file-sharing programs an inappropriate action? Why or why not?

4. Can you think of any real world situations similar to this one?

5. Which of the 10 Commandments of Computer Ethics does this relate to and why?

Closing:

Regardless of what you've heard, downloading music, programs and videos is illegal and a violation of copyright law. Music companies have already cracked down on pirating music, and it's only a matter of time before it's gone for good or you get caught doing it. However, being caught has no bearing on whether an act is moral or legal or not. And you can't use the, "But everyone else is doing it," excuse either. Not everyone is.

Steve's Shareware Secret

The Situation:

Steve downloads a game from the Internet that is shareware, meaning it can be legally used for only thirty days and then must either be deleted or purchased. If he does purchase the program, special features will be added to the game. If he doesn't purchase it then he can't play the game at all, but Steve also finds out that he can change the date on his computer so he can still play the game for free whenever he wants.

Questions:

1. What is the property? Who is its owner?

   _____

   _____

2. What happens if Steve decides to keep using the program? If he doesn't?

   _____

   _____

3. What is the advantage to the user for paying for shareware?

   _____

   _____

4. It there something in the real world that is similar to this?

   _____

   _____

5. Which of the 10 Commandments of Computer Ethics does this relate to and why?

   _____

   _____

Strong Current

Association of Shareware Professionals—

http://www.asp-shareware.org/

This website has an excellent FAQ to answer all your questions about shareware.

Comments:

Software is divided into three categories: freeware, which can be used without buying it for as long as you want; shareware, which can be used for only a certain period of time before it has to be erased or bought; and commercial software, which must be purchased before you can use it. Learning about shareware is a good way of understanding why buying software actually does benefit you. The profits that software producers make are used to develop more programs, such as expansion packs or sequels to the games you already love.

Protecting Yourself from Shark Attacks

You're probably wondering just who would really want to attack your computer and why. Hackers may not care about who you are, but they still want to gain access to your computer to use it to attack other computers or take your personal information to use against you. Being able to control your computer allows hackers to keep their locations secret while they attack other computers. Even if your computer is connected to the Internet for only a short time to talk to friends or to send email, you may still be a target. Being online for even a short time gives hackers the chance to take enough information to steal your identity or cause damage to your or someone else's computer.

There are four major types of attacks to your computer: **environmental natural**, **environmental manmade**, **human intentional** and **human unintentional**, as well as the two major vulnerabilities associated with computers, which are **through your operating system (OS)** and **through your Internet connections.**

Environmental natural attacks can best be thought of as attacks caused by Mother Nature, like floods, earthquakes, tornadoes, hurricanes, and lightning.

Environmental manmade attacks occur when people give Mother Nature a helping hand in attacking computers, and include radioactive leaks, fires caused by arson, broken water pipes, fuel line ruptures, gas leaks, and climate control failures.

Human intentional threats occur when someone purposely damages property or data, including identity theft, espionage, and credit card crime.

Human unintentional threats basically include the unauthorized or accidental change of software.

Once you've identified the type of attack, you then need to be able to determine how your computer is vulnerable to those attacks. The two main vulnerabilities to home users are to your **operating system** (OS) and to your **Internet connection**.

An **Operating System**, like Windows and Mac O/S, is the program that controls what happens inside your computer and how it reads outside devices like your mouse, keyboard, monitor, scanner, printer, etc. The older the OS, the more likely the chance it's not as secure, making it more vulnerable to attacks. If someone knows what OS you're running on your computer, the he'll be more likely to access your system and attack it. Make sure that you frequently check for security patches and updates on the main Web site of your OS.

Internet connections, whether through broadband connections like cable modems or Digital Subscriber Lines (DSL) or dialup services, are also vulnerable to attacks to your

computer. Broadband connections are more vulnerable than dialups because they're always connected to the Internet, making it easier for people to find you and take your information or send you a virus.

Once these attacks can be identified, however, your work is not done because it's up to you at that point to find the vulnerabilities in your computer and find ways to keep these attacks from occurring.

There are three common countermeasures that you can easily implement on your home information system:

Technical: Technical countermeasures mean using some sort of software to protect your system. This could include installing **firewalls** and **anti-virus software**, as well as taking steps like changing the security settings of your Web browser.

Procedural: Procedural countermeasures are any activities that you would create in order to stop attacks on your computer. This would include setting times to run your anti-virus program, password protecting your OS, and storing your important data on disks in a separate location.

Policy: These are rules used to state just how to correctly use your computer. This could be anything from keeping a list of things to do and not to do near your computer to making up your own handbook with your parents of how to properly keep your computer safe.

Strong Current

How Firewalls Work by Jeff Tyson—

http://computer.howstuffworks.com/firewall.htm

This site explains what firewalls are and how they block attacks to your computer.

Attacks and Countermeasures

Directions:

Match the attack first with which of the four types it is and then with the appropriate countermeasure for the attack.

Example:

Attack	Type of Attack	Countermeasure
Email Virus	Human Intentional	Technical

Types of Attacks	Countermeasures
Environmental Natural	Technical
Environmental Manmade	Procedural
Human Intentional	Policy
Human Unintentional	

Attack	Type of Attack	Countermeasure
Little brother keeps accidentally using sister's account		
Power surge		
Someone asks you for your password		
Extreme summer heat		
Inappropriate email		
Hackers		
Mom keeps erasing disks without checking them		
You're sent a file that attacks Windows		
Your sister keeps leaving the computer connected to the net		

The Safe Places to Surf

Now that you know more about how the Internet works, how to browse the Web, send email, chat with friends, use the Internet ethically, and protect yourself from attacks, it's time to get out there and surf!

But before you go, here's a list of sites that might interest you or help you out on that next school project or paper. Even more sites can be found at:

http://www.cerias.purdue.edu/education/k-12/6-12_Resources/

History

1st Headlines
This site provides a great collection of current event articles. The site uses several different news sources to provide a detailed look at the day's events.
http://www.1stheadlines.com/

David Rumsey Map Collection
This site features an amazing collection of historical maps.
http://www.davidrumsey.com/

Ellis Island: A History
This site provides information about how immigrants were treated, the types of conditions they faced, and the motivation for the journey.
http://www.libertystatepark.com/history1.htm

History of Costume
Looking for a great costume to use in a play or wear to a party? Then this site is the one for you. It contains graphical images of popular costumes dating from the times of ancient Egypt.
http://www.siue.edu/COSTUMES/COSTUME1_INDEX.HTML

How Far Is It?
This service uses data from the US Census Bureau and a supplementary list of cities from around the world to find the longitude and latitude of two places, and then calculates the distance between them (as the crow flies).
http://www.indo.com/distance

Jefferson's Blood
This is an amazing site that supplements the Frontline documentary on the relationship between Thomas Jefferson and Sally Hemmings. Full of dramatic video clips and images! Content is for an older student population.
http://www.pbs.org/wgbh/pages/frontline/shows/jefferson/

Legends of Pirates
If you are interested in the stories of

pirates (both the myths and facts) this is the site for you. It is a collection of great sites on the topic of pirates, buccaneers, and privateers.
http://www.legends.dm.net/pirates/index.html

Letters From an Iowa Soldier in the Civil War
See what the war was like through the letters and feelings of an ordinary soldier.
http://www.civilwarletters.com/home.html

National Geographic for Kids
This site offers all kinds of fun and interesting things for kids to check out. It is updated frequently, so check back often.
http://www.nationalgeographic.com/kids

PBS: Great American Speeches
On this site, PBS has collected over 80 years of political speeches and contains sound bytes, trivia, and images.
http://www.pbs.org/greatspeeches/

POTUS: Presidents Of The United States
On this site you can find out virtually anything you ever wanted to know about US Presidents.
http://www.ipl.org/ref/POTUS/

The History Channel
This site provides an outstanding way to connect media and history. Also, this site provides timely trivia quizzes and basic information. Excellent even if you are not looking for a TV based lesson.
http://www.historychannel.com/

This Day in History
This location provides a unique collection of historical vignettes.
http://www.historychannel.com/historychannel/thisday/

US Supreme Court
This is the official site to the highest court in the United States. Features many great resources and useful links.
http://www.supremecourtus.gov/

USA TODAY Education
The mission of USA TODAY Education is to increase the use of USA TODAY - and its targeted resources as premiere, relevant education tools for students, parents and teachers. As a result of this mission, the site provides an enormous amount of resources for teachers and students.
http://www.usatoday.com/educate/home.htm

Vikings!
Sponsored by the Smithsonian Institute, this site features a wonderful collection of images, information, and maps of the lives and adventures of Vikings!
http://www.mnh.si.edu/vikings/start.html

Voices of the Oregon Trail
Voices of the Oregon Trail an excellent website that accompanies the PBS documentary on the life of women on the Oregon Trail. http://www.opb.org/womensvoices/

World Skip
A very easy to use index of websites from countries around the world. Choose a country from a specific region to find information about local news, business, economics, travel, and activities. http://www.worldskip.com

Science

A Century of Physics
This site provides a wonderfully detailed timeline of the accomplishments in the world of physics! http://timeline.aps.org/APS/index.html

Amusement Park Physics
This online resource introduces the science of amusement park rides, including weightlessness, hills and dips, and the physiological effects of acceleration. http://www.learner.org/exhibits/parkphysics/

Cells Are Us
How did you grow from one cell? This site explains how we developed from one cell and how our bodies are made of billions of cells. The authors use fun cartoon animations to explain topics such as fertilization and cell division. http://www.icnet.uk/kids/cellsrus/cellsrus.html

eNature
This site is full of information and images that focus on all parts of nature. http://www.enature.com

Math Ideas for Science Fair Projects
This is a great listing of potential science fair or classroom projects. http://mathforum.org/teachers/mathproject.html

NASA Quest
A website "dedicated to bringing NASA people, space, and science to classrooms through the Internet. http://quest.arc.nasa.gov

NASA's Educational Program
NASA's space missions provide much information that can be easily incorporated into a classroom environment. http://www.nasa.gov

Ocean Photos
Do you like fish? Would you someday like to explore the bottom of the ocean? This site will show you what it's like ahead of time. http://www.oceanphotos.com

Solar System Simulator
This site represents a collaborative project of NASA, the Jet Propulsion Laboratory (JPL), and the California State Polytechnic University. It

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

provides to its users a "spyglass on the cosmos" and can create a color image of any planet.
http://space.jpl.nasa.gov

SpaceKids.com
This is a really fun site that will interest and teach kids of all ages about space. There are several activities, stories, and space facts.
http://www.spacekids.com

The Natural History Museum of London
This site, designed for middle and high school students, includes a variety of interactive science activities. This is definitely an "interactive" website!
http://www.nhm.ac.uk/interactive/index.html

Volcano World
This site is designed for anyone who has a special interest in volcanoes. While visiting this site you can ask a vulcanologist a question, view the most recent eruptions, find out about volcano-related conferences, locate lesson plans, and more.
http://volcano.und.edu

English

Bartlett's Quotations
Looking for something to say? Trying to add a little pizzazz to a paper? Try your hand at the words of old.
http://www.bartleby.com/99/

Classic Literature Online
Are you looking for some great books to read? This site will help you to find them.
http://www.acs.ucalgary.ca/~dkbrown/storclas.html

Folklore, Myths, and Legends
This is a huge collection of stories, legends, and common myths. It also contains a collection of related links.
http://www.acs.ucalgary.ca/~dkbrown/storfolk.html

Online Writing Lab (OWL)
If you need help with your writing, Purdue University's Online Writing Lab is available 24 hours a day. The OWL offers resources on writing skills, ESL, and career resources such as cover letter and resume writing. Over 125 handouts on writing skills are available as well.
http://owl.english.purdue.edu

Saxon Shore
Do you like the story of King Arthur and Camelot? Then you definitely want to check out this site. It is full of maps, information, and a great picture gallery.
http://www.pitt.edu/~jegst61/shoreframes.html -

The Grammar Gorillas
Part of the FunBrain.com network, this site helps students to learn to identify the different parts of speech in a fun, interactive way. Many other activities can also be accessed

through this site.
http://www.funbrain.com/grammar

Math

ARITHMETIC
Looking for ways to have fun with math? Need a little practice on your math skills? Accomplish both by checking out this site.
http://members.aol.com/_ht_a/iongoal/index.htm

Ask Dr. Math
Question and answer service for K-12 students and their teachers.
http://mathforum.org/dr.math/index.html

Cool Math
This is a wonderful resource for learning, applying, and having fun with mathematics. The site does an excellent job of emphasizing a fun approach to math.
http://www.coolmath.com

Math Ideas for Science Fair Projects
This is a great listing of potential science fair or classroom projects.
http://mathforum.org/teachers/mathproject.html

The Universal Currency Converter
This site will instantly convert currency in varying amounts and denominations. Great for math or a culture unit!
http://www.xe.net/ucc/

Fine Arts

Free Patterns
Are you crafty? Do you like to sew or stitch? This site offers free patterns for an extensive collection of hobbies. Great for classroom projects! NOTE--this site DOES request personal information.
http://www.freepatterns.com/

History of Costume
Looking for a great costume to use in a play or wear to a party? Then this site is the one for you. It contains graphical images of popular costumes dating from the times of ancient Egypt.
http://www.siue.edu/COSTUMES/COSTUME1_INDEX.HTML

Internet Movie Database
This is an excellent site for finding out more about movies or actors. Information includes: filmographies, awards, plot summaries, trivia, box office grosses, and everyone who was involved in the making of that movie. http://www.imdb.com/

Rock and Roll Hall of Fame
This is a great site to visit to check on the roots of Rock and Roll.
http://www.rockhall.com/

Sapphire Swan Dance Directory
This site contains a wonderful collection of links to sites that focus upon all types of dancing.
http://www.SapphireSwan.com/dance/

APPENDIX C:
RELATED MATERIAL FOR GOAL 3

The Center for Education and Research in Information Assurance and Security
Purdue University ● 656 Oval Drive ● West Lafayette, IN ● 47907-2086
(765) 494-7871 ● Fax (765) 496-3181 ● k-12@cerias.purdue.edu ● www.cerias.purdue.edu

CERIAS Workshops for the K-12 Technology Coordinator

Intended Audience

Technology coordinators and/or school administrators who are responsible for information security, including policy development, in a school or school system.

General Abstract

An unfortunate perception about information security is that it is just about protecting computers. Many factors affect information security, and not all of them concern the technical aspects of computers and networks. In fact, the practice of information security transcends many aspects of an organization and is actually on of the most critical policy and structure decisions in any school system.

To ensure the security of a school's information, the availability of services critical to learning, and the safety of a school's constituents, administrators and technology staff need to stay apprised of fundamental security concepts and procedures, current and emerging security practices, and the theory that serves as the foundation for sound security decisions.

Purdue University ● 656 Oval Drive ● West Lafayette, IN ● 47907-2086
(765) 494-7871 ● Fax (765) 496-3181 ● k-12@cerias.purdue.edu ● www.cerias.purdue.edu

Workshop 1: Security Foundations & Risk Analysis

Description

This one- or two-day course will provide you with an overview of the foundational principles and goals of a sound information assurance and security program. In order to understand the policies, procedures, guidelines, training, and technology that your school needs to protect your information assets, you need to understand these fundamental principles. This course also demonstrates how to use cost effective risk analysis techniques to identify and quantify the threats to your organization, the origin of the threats, necessary countermeasures to reducing or eliminating the threat, and associated costs.

Objectives

- Recognize the purpose & value of information security.
  Understand and prioritize information security goals.
- Use basic information security terminology.
- Understand the purpose of information security risk analysis and its relationship to risk management.
- Recognize the benefits, types, and scales of risk analysis.
- Understand and practice the steps of risk analysis.

Workshop 2: Creating & Auditing School Security Practices

Description: Many people perceive information security to be a technology problem, when in fact technical solutions alone cannot achieve information security; information security decisions impact organizational policy and culture, and thus need to address the human components of a program. The cornerstone of an effective security architecture is well-written policy. This one- or two-day course demonstrates how to develop effective policies, practices, guidelines, and procedures that mitigate your school's information security risks. After completing this course, your school should be better prepared to establish a program that protects your information resources and guides personnel behavior.

Objectives:

- Use results of a risk assessment, in conjunction with security best practices, to develop an information security policy.
- Create and audit information security practices in order to determine the effectiveness of the information security program in place in the local school system.
- Identify the people, technology, and processes model for information security practices.
- Apply the people, technology, and processes model to the local school system.
- Describe and apply steps for evaluating security practices.

Workshop 3: Developing and Implementing a Security Training and Awareness Program

Description: Have you ever heard the phrase "employees are your best firewall?" This statement strikes at the heart of the information security problem; too often, information security programs fail because they address only the technological issues. This one-day course will highlight how to conduct security awareness training and initiatives that impact user behavior and makes your school's computer users one of the most effective countermeasures in your information security program.

Objectives:

- Conduct a gap analysis to identify poor security practices common to computer users.
- Identify practices and issues relevant to the K-12 population.
- Analyze successful and failed awareness and training programs.
- Develop goals for an awareness and training program.
- Select appropriate training and awareness interventions for your computer users.

Workshop 4: Intrusion Detection Systems

Description

While many technology coordinators and system administrators are comfortable with implementing firewall technology, there are many unanswered questions about an equally important security technology, intrusion detection systems. Intrusion detection systems include technological mechanisms, written security policies, and procedures used for detecting unauthorized system use. This one-day course will demystify intrusion detection systems by explaining the underlying basics of intrusion detection, providing further insights into the technology, and describing current limitations so that technology coordinators and system administrators will be able to effectively purchase and implement the intrusion detection system that is right for their school.

Objectives

- Describe the basic functions, goals, and uses of an intrusion detection system (IDS).
- Compare an IDS to other security technologies, including a firewall.
- Describe the types of IDSs.
- Weigh the advantages and disadvantages of implementing and maintaining types of IDSs.
- Understand/decrypt IDS vendor terminology.

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu

Keeping Information Safe: Practices for K-12 Schools

Abstract

K-12 educators and support staff are largely unaware of the threats and vulnerabilities associated with the information systems they use. For example, confidential and sensitive information can be stolen, lost, and exposed to the public. This threat is especially pertinent to Indiana educators and support staff, who are obligated to protect sensitive information such as Student Test Numbers under the Family Educational Rights and Privacy Act, or FERPA, which is one of the nation's strongest privacy protection laws. These individuals need opportunities to learn about the threats and countermeasures associated with information protection.

To improve the technological and information security literacy in K-12 schools in the state of Indiana, the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University wishes to develop an end-user training and awareness program targeted at pre- and in-service K-12 educators and support staff.

This proposal was written specifically for the repurposing of an existing set of modules to better suit the K-12 audience and address information protection needs specific to the K-12 audience. This proposal will fund necessary work to modify existing content, exercises, case studies, and assessment mechanisms to better suit the K-12 audience, as well as the technical development, evaluation, and dissemination of the modules both in courses at Purdue University and throughout K-12 schools in the state of Indiana. Two populations will be served: The primary audience is 1) in-service K-12 educators who hold a bachelor's degree or higher in education or a related field and 2) K-12 support staff who operate computers as end-users and/or handle sensitive and confidential information. Beginning in the summer of 2004, this audience will have the opportunity to learn about protecting information by experiencing "Keeping Information Safe: Practices for K-12 Schools."

The secondary audience consists of participants in the Purdue University undergraduate teacher education program. "Keeping Information Safe: Practices for K-12 Schools" will be used in conjunction with teacher education courses taught on campus, including EDCI 270, Introduction to Educational Technology and Computing; EDCI 271, Classroom Applications of Educational Technology; and EDCI 564, Integration and Management of Computers in Education.

Purdue University ● 656 Oval Drive ● West Lafayette, IN ● 47907-2086
(765) 494-7871 ● Fax (765) 496-3181 ● k-12@cerias.purdue.edu ● www.cerias.purdue.edu

PURDUE
UNIVERSITY

The Center for Education and Research in Information Assurance and Security

Purdue University • 656 Oval Drive • West Lafayette, IN • 47907-2086
(765) 494-7871 • Fax (765) 496-3181 • k-12@cerias.purdue.edu • www.cerias.purdue.edu