Your complete guide to

Teaching Cyber Safety to the Digital Generation

Inside, you find out …

• How to talk to kids about online safety
• How to avoid personal information exposure
• How to educate students on cyberbullying
• What types of activities you can use with your students

Nancy Muir has taught Internet safety courses at two major universities and runs a Web site on seniors and computing (techsmartsenior.com). She is the author of over 60 books on technology topics and a Vice President at LookBothWays—a company specializing in Internet safety education. Nancy also writes a regular column on computers and the Internet at Retirenet.com.

Visit us online at CliffsNotes.com

Guide to

Teaching Cyber Safety to the Digital Generation

A resource written specifically for teachers

Nancy Muir

Learn more on the Web

www.Dell.com/K12
www.Microsoft.com/education
CliffsNotes®
Guide to Teaching
Cyber Safety to the
Digital Generation

By Nancy Muir

Wiley Publishing, Inc.

These materials are the copyright of Wiley Publishing, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.
Table of Contents

Introduction .............................................................. 1
    How to Use This Book ........................................... 1
    Icons Used in This Book ........................................ 1
    Transforming Education for the Digital Generation ........... 2
        Dell ................................................................. 2
        Microsoft ........................................................ 2

Chapter 1: Talking to Kids about Online Safety ...................... 3
    How Old Should They Be? ........................................ 3
    Learning about Types of Online Sites ......................... 5
    Why Online Risks Exist ......................................... 6
    What Are the Risks? ............................................. 7
    What Can You Do? ................................................ 8
    What Can Your School Do? ..................................... 8

Chapter 2: Practicing Safer Internet Browsing ......................... 11
    Safe Searching Practices ....................................... 11
    Consider What Drives “Free” Online Sites .................... 12
    Avoiding Download of Malware ................................ 12
    Setting Pages to Private ........................................ 14
    Be Cautious about Uploading Images .......................... 15
    Discover Risks of ID Theft and Financial Scams ............ 16
        Checking your credit ......................................... 16
        Fishing for fraud ............................................. 17
        Recognizing Predatory Behavior and Its Effects .......... 18

Chapter 3: Considering the Permanence of Online Information ...... 21
    Understanding You Are Not Anonymous ....................... 21
    Information Accumulates ....................................... 22
    Others May Not Be Who They Claim to Be .................... 23
    Employers and Schools Consider Online Information ......... 24
    Using the Internet to Build a Good Reputation ............... 25

Chapter 4: Getting a Handle on Cyberbullying ......................... 27
    Why Is Cyberbullying a School Issue? ....................... 28
    How Does Cyberbullying Hurt Victims? ....................... 29
    How Does Cyberbullying Hurt Bullies? ....................... 30
    How to Deal with a Cyberbullying Situation .................. 30
Chapter 5: Ten Great Online Safety Web Sites ......................... 33
  iLookBothWays.com ............................................. 33
  SafeInternet.org ......................................................... 33
  WiredSafety.org ......................................................... 34
  InternetSafetyEducator.com ......................................... 34
  SafeKids.com .......................................................... 34
  Coolcatteacher.blogspot.com/index.html ............................ 34
  FBI Parents Guide ........................................................ 34
  Netsmartz.org and Netsmartzkids.org .................................. 35
  iKeepSafe.org .......................................................... 35
  CommonSenseMedia.org/educators ...................................... 35

Chapter 6: Ten Tips for Creating Strong Passwords .................... 37
  Make It Longer ........................................................... 37
  Use Variety ............................................................... 37
  Don’t Include Personally Identifiable Information ................... 38
  Avoid Repeated Letters or Numbers ................................... 38
  Avoid Common Words ................................................... 38
  Spell Words Backwards .................................................. 38
  Keep Passwords in a Safe Place ......................................... 39
  Change Pass Phrases Often ................................................ 39
  Don’t Use the Same Password Everywhere ................................ 39
  Be Cautious about Password Hints ....................................... 39

Chapter 7: Ten Guidelines for Safer Buying and Selling Online....... 41
  Choose the Best Payment Method ........................................ 41
  Use Stores You Know ..................................................... 42
  Identify Trusted Online Sites ............................................. 42
  Deal Locally with Classified Ads ......................................... 42
  Use Sites with Secure Transaction Technology ....................... 43
  Don’t Let People Come to Your Home .................................... 43
  Don’t Hand-Out Your Password ........................................... 43
  Use the Protection of the Auction Site .................................... 43
  Delete Your Personal Information ........................................ 44
  Watch Your Costs ......................................................... 44

These materials are the copyright of Wiley Publishing, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.
INTRODUCTION

Digital technology is a central part of most kids’ lives today, and a fantastic tool for educators. As digital devices and programs become more prevalent in the classroom, responsible teachers are concerned with educating kids about how to be safe using those technologies. This book helps you understand how to talk to kids about online safety, how to explain the types of risks and how to avoid them, and how to help students who have been victimized online.

I’ve tried throughout to flag particular concerns by age group. No matter what grade you teach, this book should prove helpful.

How to Use This Book

For the most part, the chapters in this book aren’t presented in any sequential order, meaning you can jump in anywhere that suits you. Here’s a rundown of the chapters.

Chapter 1: This book starts off with an overview of risks and ideas for how to talk to kids about online safety.

Chapters 2 through 4: These chapters address three key facets of online safety: risks when browsing, ways to avoid personal information exposure, and the nature of cyberbullying. You can move among these chapters in any order based on what your focus is at the moment, but reading them all will give you a much better grounding in online safety.

Chapters 5 through 7: The last three chapters provide quick lists to help you find additional information, learn about how to create strong passwords, and help students understand how to become smarter online consumers.

Icons Used in This Book

You will see a Tip icon used throughout this book. Tips offer advice or a way to further explore a topic.

This icon relates to points that are worth reinforcing, because they are key to online safety.

Warnings alert you to potentially dangerous online behavior or serious risks.
Transforming Education for the Digital Generation

Kids are growing up in the digital age. They communicate, collaborate, and learn differently than previous generations, with the Internet at the center of most technology interaction. As teachers, parents, and technology partners with the education community, everyone must take an active role in helping children use Internet access and technology safely, effectively, and intelligently.

Together, Dell and Microsoft are sponsoring this publication to help develop students’ critical thinking skills around cyber safety. This book provides practical advice on teaching your students to be responsible as they develop lifelong learning skills for a digital age.

Dell

By infusing technology and Internet access into the classroom environment, teachers have an opportunity to engage students in new ways and enhance the learning process. At Dell, we believe technology can help students reach their highest potentials.

Dell’s Connected Classroom solution empowers educators with the latest tools and professional development necessary to help engage students, differentiate instruction, and teach the 21st century skills needed to succeed in this digital age.

Find out more about Dell and education at www.dell.com/K12.

Microsoft

The evolving demands of the global economy make education vital to sustainable social and economic success. Education is a fundamental human right and is the single most important investment in the future of individuals, communities, the nation, and the world.

Microsoft works with local, national, and international education communities to create technology, tools, programs, and solutions that help address education challenges, while improving teaching and learning opportunities. We hope that technology can help extend powerful new education opportunities to millions of people.

Discover more information about Microsoft and education at www.microsoft.com/education.

These materials are the copyright of Wiley Publishing, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.
Chapter 1

TALKING TO KIDS ABOUT ONLINE SAFETY

Chapter Check-in

❑ Realizing online safety is about behavior, not technology
❑ Knowing what online behavior leads to risks
❑ Protecting personal information
❑ Understanding risks and changing online behavior

Parents and educators often struggle with the idea of teaching kids about online safety. “Kids are so much more on top of technology, and they tune me out when I try to teach them anything about the Internet,” is a sentiment I hear often.

The basic flaw with that excuse is that online safety is seldom about technology; rather, it’s about behavior. The choices you make about what information to share, with whom you will interact online, and where to place your trust as you browse the Internet are key to staying safer. If you consider that you have much more experience with making those types of judgments than your students, it’s a natural for you to help educate them in how to stay safer online.

Above all, don’t make your online safety program a series of don’ts. Instead, empower your students to make intelligent choices and discover what they can do with technology to help them be more successful in their education, personal, and work lives.

How Old Should They Be?

It’s never too early to begin to teach online safety. As soon as a child has access to a computer, you can begin to help him or her develop safer
online habits. In fact, it’s best to teach safety at a younger age when children are more accepting of authority and when they are learning how to stay safe in the offline world. Do what you can to get online safety education into the early grades in your school system.

What if you’re starting with older kids? Remember, you can’t force online safety on older kids—they will find a way around restrictions and filters. Instead, make them partners in keeping themselves and others safe. Though most older kids think they know it all, you find some interesting information in this book to share with them that may surprise—and impress—them.

Think of it this way: When kids are taught to lock the door to the house at night or to use caution crossing the street, they don’t object. It makes sense to them because nobody likes to be hurt or ripped off. Show them the self interest in learning how to behave safely online, and they will get it, every time.

Not every age group is at risk for the same things. Based on the technologies and devices available to them (for example, a personal cellphone) and the tendencies of their age group to follow rules or fly in the face of them, they face different issues.

Table 1-1 sums up the greatest risks by age group.

<table>
<thead>
<tr>
<th>Age Group</th>
<th>Major Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grades 1–4</td>
<td>Clicking on a link that downloads malware</td>
</tr>
<tr>
<td></td>
<td>Stumbling upon inappropriate sites</td>
</tr>
<tr>
<td></td>
<td>Sharing passwords</td>
</tr>
<tr>
<td></td>
<td>Making friends with a stranger online</td>
</tr>
<tr>
<td></td>
<td>Responding to advertising gimmicks in children’s games/social sites</td>
</tr>
<tr>
<td>Grades 5–8</td>
<td>Cyberbullying</td>
</tr>
<tr>
<td></td>
<td>Posting inappropriate images of themselves</td>
</tr>
<tr>
<td></td>
<td>Sexting</td>
</tr>
<tr>
<td></td>
<td>Flaming in online games</td>
</tr>
<tr>
<td></td>
<td>Exposing personal information on social networks</td>
</tr>
<tr>
<td></td>
<td>Exposure to sexual predators</td>
</tr>
</tbody>
</table>

These materials are the copyright of Wiley Publishing, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.
### Chapter 1: Talking to Kids about Online Safety

#### Age Group Major Risks

<table>
<thead>
<tr>
<th>Grades 9–12</th>
<th>ID theft as they apply for loans and credit cards</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Posting information/images that could damage their life choices</td>
</tr>
<tr>
<td></td>
<td>Responding to financial scams/phishing</td>
</tr>
<tr>
<td></td>
<td>Exposing emotional vulnerabilities to strangers</td>
</tr>
</tbody>
</table>

With older kids, it’s a good teaching technique to ask them to show you how to use their favorite sites, and as they do, point out safety issues to them in sites’ Terms of Service and default privacy settings.

### Learning about Types of Online Sites

Before you can understand the types of risks out there, you have to understand what types of activities are available to kids. Here are explanations of some of the most frequently-used online services and features:

- **Blog:** (short for Web log). This is an online journal which can be set to be private, or made available to a select group of people or the general public to view. Blogs appear on a variety of types of sites, and sites such as Thoughts.com and WordPress.com offer free blogs.

- **Social networking:** Social networking sites such as Facebook (see Figure 1-1) allow users to create a blog, but what really differentiates social networking sites is the ability to create a network of friends. In addition to blogging, social networks allow users to exchange virtual gifts, post pictures and videos, invite each other to events, and take and exchange surveys and quizzes.

- **Friends of Friends:** The ability to expand a network of online friends with this feature means that whoever your friend befriends, gets on your friends list, gaining access to your information. This feature is used on social networks and in instant message programs. Though kids often feel a large number of friends is cool, in fact this feature can allow lots of strangers to have access to information that they thought was private.

- **Video sharing:** Sites such as YouTube allow users to post and view videos, rate and comment on those videos, and email links to videos to others.
■ **Instant messaging (IM):** An IM program such as MSN Messenger allows real-time text conversations between users. Many IM programs provide versions that can be used on cellphones.

■ **Texting:** This is the term for sending text messages between cellphone numbers. This is nearly instantaneous communication, and one used often by young people today. Sexting is the use of this texting feature to send sexually explicit messages.

■ **Wiki:** A wiki is a collaborative site where anyone can contribute to, edit, or remove content. It is most often used in educational or work project settings. Wikipedia is one publically available wiki many people are familiar with.

**Figure 1-1** Facebook is a currently popular social networking site.

![Facebook](image)

**Why Online Risks Exist**

We live in the Wild West days of online technology. No one is in charge. Governments can’t lay claim to it and control the cross-border online population. The Internet is therefore a perfect storm for online criminals who know how to stay anonymous, shift their scams constantly to lure new victims, and escape the law.
People themselves have no rigid set of ethics about what’s right or wrong in their online behavior, and in fact often feel they are anonymous (they’re not) and so can step away from their usual code of ethics. In addition, some online tools, software, and devices contain security flaws because they’re not built with the idea of what the bad guys can do with them. They’re built for honest folks like you and me. For example, though it’s a good idea to not use your real name in your e-mail username, many e-mail services display your full name next to your username in e-mail messages by default.

The fact is that everyone is learning how this new world should operate and how we should behave in it. That’s why your role in educating kids about this new world is so important—not just to your school but to creating a more ethical global online citizenry.

**What Are the Risks?**

The most touted online risks in the press are typically sexual predation and cyberbullying, both of which can result in tragic acts. In reality, kids are less likely to become a victim of an online sexual predator than to have their IDs stolen, and cyberbullying isn’t a big concern for younger and high school-aged children: It is most prevalent in the middle school years.

That does not mean you should not learn how to spot victims of sexual predation or cyberbullying. But the sensationalized stories about Internet crimes often cast a sense of fear which stops people from taking advantage of all the Internet has to offer. Part of educating young people about online safety is to make them feel they can take control and stay safer if they learn the right lessons to take advantage of technology.

A lot of offline crime is caused by online behavior that many people are unaware of because it is hard to see the connection. Say that a kid announces on Twitter that the family has just bought a new large screen TV and is headed to Disneyland for the weekend. Most folks do not connect the dots when the house then gets robbed. It is important to keep in mind that exposing our whereabouts and financial information can make us offline targets.
What Can You Do?

Cybersafety doesn’t have to be hard to teach. By conveying a few simple guidelines, you can help your students stay much safer online. Teach them that

■ Personal information has value. Of all the things you can do online to protect yourself, limiting information exposure is by far the most important. Exposing your information to strangers enables financial scams, cyberbullying, sexual stalking, and offline crimes, such as robbery and assaults.

■ Online information is permanent. The info stays online forever providing a roadmap to your finances and emotional weaknesses and a display of your youthful indiscretions that anybody and everybody can find.

■ Predators have certain tactics that they use again and again. Discover how to spot the tactics, and you can foil attacks from sexual predators and financial scam artists alike.

■ They should get and use technology tools. These tools include antivirus and antispyware programs. They should update their definitions often and learn to create safer passwords and change them often.

■ Respect is key. Students have an obligation to treat others with respect online and demand respect from people, online companies, and those in your life who could expose you to risk.

What Can Your School Do?

Schools need to set the example for online safety. Your school and school district should consider the following ideas:

■ Have firm rules about cyberbullying and enforce them.

■ Post rules about use of computers in school.

■ Discuss what filters or restrictions for online access are appropriate, while still allowing students to get the most out of technology to help them learn and prepare for a role in the larger world.
■ Involve parents as much as possible. Share with them the information you are providing to students about online safety and encourage them to get involved with their children’s online lives.

Be aware that teachers have been dismissed for allowing inappropriate online content into the classroom. Make sure you know how to use the computers at your disposal to avoid clicking on inappropriate links and how to navigate away from inappropriate sites. Staying safe online isn’t that hard once you understand the potential risks and the behaviors and technologies that help you stay safer.
Chapter 2
PRACTICING SAFER INTERNET BROWSING

Chapter Check-in

❑ Your information is a commodity
❑ Malware can damage your computer and expose you to technology attacks
❑ Use privacy settings to protect your online pages
❑ Spot common e-mail scams
❑ Learn to recognize predatory behavior and protect yourself from it

Students often use the Internet to do research for school projects. This involves browsing among sites and using search engines, which can put them at risk of downloading malware, like viruses, or exposing their own information. In this chapter, I offer some tips for safer browsing and searching.

Safe Searching Practices

When searching the Internet, keep in mind a few things that affect your safety and your students’ safety:

- Be careful about the search terms you enter. Searches that include the world “free” turn up results that include 14 percent fraudulent sites, according to a McAfee study.

- When you perform a search, avoid clicking on sponsored results. Even though many people feel these are okay because the search
engine company is somehow endorsing these sites, in fact visiting these sites by clicking on the link in the search results is more likely to result in downloading of malware to your computer. See the section “Avoiding Download of Malware” for more information.

■ Clicking on ads on a site is never a good idea. Instead, enter the site address into your browser to go there.

Consider What Drives “Free” Online Sites
When you search for free mortgage calculators or click on a link for a free game, how do you think the people at the other end of the link pay for what they give you? It’s simple: They sell you to advertisers. You may feel that entering your income and other financial information in an online calculator is anonymous, but it may not be; it may make your information available to salespeople or phishing scammers.

Even legitimate businesses may earn more from selling your information than the advertising space they sell to others businesses. A major search engine company is expert at data mining (compiling information about peoples’ online habits) and selling information to others. A prominent social networking site states in its terms that it owns any content you post, even after you cancel your membership. Some of this activity may be fine by you—it allows a business to know how and what to market to you. Other uses of your information can put you at risk or open you up to spam and annoying pop-ups.

Tip
Have your students examine the terms of a popular social networking site and see what rights that site has to the content they post. When kids find out that “their space” isn’t really theirs, they often get outraged. After they learn the lesson that nothing is free online and that the free services they use do have a price, they can make informed decisions about which online features to use and which to avoid.

Avoiding Download of Malware
One of the most prevalent dangers online is the risk of downloading damaging programs called malware. Malware is the collective name for programs that can take a variety of forms:

These materials are the copyright of Wiley Publishing, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.
Chapter 2: Practicing Safer Internet Browsing

- A virus is a program that can be spread via the Internet and infects computers. Most often it attacks the data on your computer or makes changes to your system settings that hurt your computer’s performance.

- Spyware includes programs that track your online activities. This information can be used to sell to you, or to sell information about your activities to others.

- Adware gets downloaded to your computer when you visit certain sites and causes pop-up windows to appear selling you things. Adware can also slow down your computer’s performance.

- Keystroke logging software, once downloaded to your computer, can allow someone to remotely track your every keystroke. When you go to your online bank and enter your user name and password, for example, keystroke logging software makes that valuable information available to a criminal in a remote location.

- Worms, Trojans, and Rootkits are other types of malware whose focus is to gain access to your computer system or a computer network.

Teach kids to avoid malware with a few simple steps:

- Get and use antivirus and antispyware software that can detect and prevent the download of malware. Update the software frequently so it can catch the latest malware threats.

- Avoid clicking on links, especially in advertisements and e-mails.

- Avoid downloading and running attachments to emails if they are executable files (these have a file extension of .exe at the end of the file name which is the file format used by a virus).

- Get a program such as McAfee Site Advisor or AVG, which alerts you to dangerous sites in search results, and never visit sites they flag as dangerous.

If you teach middle-school or high school, assign a research project to have students compare the features of various anti-virus and spyware programs. Are free programs as good as programs that charge a yearly subscription fee?
Get any updates to an operating system such as Microsoft Windows as they become available. These updates typically contain fixes to security flaws that could help protect your computer from malware.

Younger kids are especially prone to clicking on a cute animated ad for a free trip to Disneyland or a free toy. These almost invariably take them to sites that download malware to the computer. Find safe sites for them to visit and tell them to stay within those sites and not click on links or ads.

**Setting Pages to Private**

Your students probably all have pages on one or more social networking sites. These sites offer wonderful opportunities for socializing and sharing, but they also encourage users to post a ton of personal information (that could later be misused by the wrong people). Cyberbullies get ammunition from these pages for their attacks. Companies get information to market their products. Crooks get information that tells them when a house full of wedding gifts will be left vacant during a honeymoon. Sexual predators get personal information they can use to groom a victim.

If you want to be safer on social networking sites, follow this advice:

- By default during the sign up process some sites set pages to be publicly available and encourage new members to invite many people to be their friends so they will be more popular. Figure 2-1, for example, shows how unsolicited suggestions of friends to add to your account are sent to you regularly. Setting a page to be private and only inviting people they know offline to be friends is the safest practice.

- Avoid creating a username that is provocative or reveals identity. For example:
  - *SweetNHHotGirl* invites the wrong people and suggests this is a young female.
  - *94GarfieldJock* may reveal date of birth, school or town, and possibly gender of the member.

- Avoid posting blog content that reveals your location (such as your address when talking about an upcoming party), your phone number, or after-school activities and times. Your friends know these things, strangers don’t need to.

These materials are the copyright of Wiley Publishing, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.
Figure 2-1 Many social sites actively encourage adding friends.

- Remember that even with a site set to private, certain information is shown in your publically available member profile, such as your username, town, and photo.

- Social sites for very young children are rife with hidden advertising. Even young kids get it when you explain that, though the site says it’s free of advertising, they are frequently encouraged to buy T-shirts, games, virtual gifts, and so on. Smart online consumerism starts early.

Middle schoolers are at that stage in their lives when they begin expanding their circle of acquaintances and testing limits. They are therefore most at risk to sexual predation as they create wider circles of online friends. Teach them that a friend of a friend is a stranger and that people can represent themselves to be anyone they wish online, with a variety of motivations.

**Be Cautious about Uploading Images**

A picture truly is worth a thousand words to an online predator. If a child uploads an image of himself standing in front of his house, with the house number and street sign showing, wearing a school team shirt, a criminal or predator can find a wealth of information. What’s shown in a photo may reveal:

- Location

  - Economic status

These materials are the copyright of Wiley Publishing, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.
It’s important that kids understand how posting images can reveal information that can put them at risk. In addition, posting provocative pictures or pictures that could prove embarrassing if unearthed in a search by a school, employer, or potential mate is simply not a good idea.

Have students bring in photos of themselves and see how many clues the class can find about where they live or what their activities are. This practice may help them understand how photos they post online help predators target them.

**Discover Risks of ID Theft and Financial Scams**

Many people are surprised that even infants and young children have their identities stolen. Visit any baby announcement site and you’ll find information about a child’s name, date of birth, parents’ and grandparents’ names, where they live, and more details that make them targets for ID theft. False passports can be based on such information and sold for a pretty penny.

**Checking your credit**

As a child gets older, he or she begins to build a credit record. At some point kids will obtain a credit card or apply for a student loan. It’s at this point that ID theft can escalate.

From about 14 years of age and on, kids should know how to obtain a free credit report and protect their credit with steps such as a credit freeze, which stops anybody for applying for credit in their names. The site [www.idtheft.gov](http://www.idtheft.gov) (see Figure 2-2) provides more information about these important steps.
Chapter 2: Practicing Safer Internet Browsing

Figure 2-2 This government site provides advice on avoiding or coping with ID theft.

It’s important to teach high school age kids about how to protect their finances with tools such as credit freezes. They should know that the biggest risk to their finances isn’t that somebody will hack into their bank account and steal a few hundred dollars; it’s that someone could apply for tens of thousands of dollars of credit in their name and ruin their financial future.

Fishing for fraud

Students should also be taught to recognize fraudulent e-mails called phishing scams. These e-mails often claim to be from financial institutions. Sometimes they ask for an account number or password. Other times they offer a link to click to avoid having the account shut down.

Most of these scams have certain things in common:

- They demand quick action: Click here now so your account is not shut down; verify your account number so we can offer you this incredible new credit card before the promotion expires; and so on.

- They repeatedly ask you to click links. These links may take you to a site that downloads malware but is just as likely to take you to a phony site that requires you to use your account user ID and password to log on. You have just given that information away to crooks.

These materials are the copyright of Wiley Publishing, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.
Phishing e-mails may look authentic at first glance, but study them for typos, misspellings, and poor grammar. These issues are often a giveaway.

If you check the e-mail sender’s address it may seem to come from a financial institution, but study it carefully or right-click on a link to see its real properties. An e-mail from Joe@PayPalCentral.net may seem to be from the PayPal payment service, but PayPalCentral does not exist. A link that leads to FirstFederalBankAuthority.au.net does not take you to First Federal Bank, and the .au in the address indicates you’re going to a site set up in a foreign country.

Check out Figure 2-3 for an example of a phishing scam.

Figure 2-3  A typical phishing scam.

Recognizing Predatory Behavior and Its Effects

As Linda Criddle, an expert in online safety (iLookBothWays.com), discerned from studying predators in prison over several years, certain patterns to predatory behavior surface again and again. Recognizing these behaviors can help anybody avoid becoming a victim.

Predatory behavior, called grooming, includes

- Befriending a person by citing common interests (interests which can be discovered in online postings)
Gifting behavior. Online this practice may simply involve presenting the victim with a virtual bouquet of flowers, or offline, sending gifts to the home.

Separating the victim from family and friends by sympathizing with a rant about an unfeeling mother or negligent friend.

Making the victim feel loved, causing that person to love the predator in return.

Making the victim feel guilty: You caused me to behave this way, you wanted it, and so on. This tactic makes the victim frightened to report the behavior to others because the victim feels responsible for the situation.

You can often spot signs of somebody who is being stalked by a predator. These signs include the following:

- The person becomes withdrawn.
- He receives calls at odd times of the day.
- She receives gifts from people you don’t know.
- Your student begins to isolate himself from friends and family as the predator draws him into the new relationship.

The key to helping somebody who has become a victim of an online predator is to make that person feel that it is not her fault. She should know that others want to provide support. This support helps to overcome any fear of punishment for what she has come to believe is partially her fault.

If a child receives a disturbing online communication and reports it to you, don’t disconnect from the Internet thereby losing the communication. Instead, turn off the monitor for the moment, but go back and save the communication when the child has calmed down and is out of range of the computer. Such communications can be used as evidence when contacting law enforcement to report inappropriate online behavior toward children.
Chapter 3

CONSIDERING THE PERMANENCE OF ONLINE INFORMATION

Chapter Check-in

❑ Understanding online anonymity
❑ Seeing how information from various online sources accumulates
❑ Discovering how your online activities are viewed by schools and employers

Help your students to understand the nature of online information. They may not realize what they’re exposing nor that the information placed online lasts forever in many cases. Actions they take online today may haunt them down the road. Protecting their information and understanding the impact it can have are two keys to a safer online future.

Understanding You Are Not Anonymous

There is an odd phenomenon at work when people go online. They consider that nobody knows who they are. They think that usernames keep them anonymous when they flame someone in an online gaming environment. They feel that their instant messages and e-mails can’t possibly be read by anyone but the recipient.

The truth is, they’re wrong. Gaming sites and social networking sites know who their members are and track their behavior. E-mails and text messages from phones can be intercepted as they travel over a network or via Bluetooth. Online companies may be exposing your identity in ways you hadn’t considered.
Make sure students realize that there are consequences to their behavior online and that inappropriate or illegal behavior can come back to haunt them.

**Information Accumulates**

Not only are you not anonymous online, but also the information about you comes from many sources and accumulates over time to produce a pretty detailed profile of you.

According to one study from Georgetown University, child bloggers typically reveal a great deal about themselves, as shown in Table 3-1.

<table>
<thead>
<tr>
<th>Table 3-1 Percentage of Young Bloggers Who Reveal Personal Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type of Information</strong></td>
</tr>
<tr>
<td>First Name</td>
</tr>
<tr>
<td>Age</td>
</tr>
<tr>
<td>Contact Information</td>
</tr>
<tr>
<td>Location</td>
</tr>
<tr>
<td>E-mail Address</td>
</tr>
<tr>
<td>IM Name</td>
</tr>
<tr>
<td>Birthdate</td>
</tr>
<tr>
<td>Link to Home Page</td>
</tr>
<tr>
<td>Full Name</td>
</tr>
</tbody>
</table>

But kids aren’t the only ones putting information about themselves out there. Ask them to consider possible sources of information about them online (even if they have never gone online themselves!):

- Your school Web site may publish pictures of you at sports or arts events with your name in the caption.
- When you’re employed, your company may publish a press release noting your accomplishments, attendance at a conference, or personal information.

These materials are the copyright of Wiley Publishing, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.
Chapter 3: Considering the Permanence of Online Information

- A local newspaper may mention you in an article about a volunteer organization or club.
- Your city government may make information about your house and property tax available online.
- A family member may make information about you available on a genealogy site.
- A friend may publish information about you in a blog on a social networking site.

The fact is that information you post combines with information posted by a variety of people. Using that collective information, criminals or companies or your government can get to know a lot about you.

Working with your students to find these types of information can be fun. Check out these activities:

- Have students do a search on their own names and see how much information may already be out there about them and from what sources. If they find information they are concerned about, encourage them to contact the hosting site and ask for it to be taken down. Not all sites will do this, but some will.
- Do an inventory of the ways in which your school may expose students. Do you protect certain information on your Web site from others, allowing only parents and students to access student pictures or activity schedules? Do you send pictures of sports teams to the local paper with member names? Although this information may not be damaging, it could reveal student identities to potential predators.

Others May Not Be Who They Claim to Be

The average computer user isn’t good at staying anonymous online, but it’s important to remember that criminals are. They can create phony Web sites that seem legitimate and appear one day and disappear the next. They can seem to be located in your community but be operating out of a country halfway around the world. They can very cheaply create e-mails from your bank or an online store that seem to be genuine, but aren’t.

These materials are the copyright of Wiley Publishing, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.
Those who pretend to be what they are not range from the individual sexual predator to organized crime. Countries host gangs of criminals who harvest data for ID theft operations on a routine basis. Collections of e-mail addresses send spam or phishing messages pretending to be your bank or a charity or an online retailer reporting a problem with your credit card.

A healthy dose of suspicion helps most people deal with these phony representations, simply using the common sense that comes into play in offline situations.

**Employers and Schools Consider Online Information**

Students need to realize that their actions online today have consequences, just as their actions do in the offline world do. Kids who would never expose their bodies or personal feelings to strangers on the street do so routinely online.

Make the point that colleges and employers now routinely perform online checks on every candidate they review. Certain companies hire out this service, and they can quite easily find past postings by students, as well as information about those people posted by others.

Tell students about these examples of posting dangers:

- Do not post or send out inappropriate pictures of yourself that are sexually provocative. (Remember a current boy- or girlfriend could become somebody who is only too glad to send out such a picture to the world in retribution for a breakup.)
- Do not post pictures or text about activities, such as getting drunk or shoplifting.
- Do not brag about cyberbullying a fellow student.
- Do not be abusive or disparaging about your teachers or employers on a public site.

Employers don’t stop with online checks when hiring. They stay alert to blogs and other postings by employees that are disparaging of their employer. People have been fired over inappropriate blogs about their
bosses or company. In addition, be sure that students know that many companies monitor their use of computers on the job. Inappropriate use of company computers for personal business is another cause for dismissal at some companies.

Companies employ monitoring software to watch their employees and what they do on their computers each day. Check out Figure 3-1 for an example of this technology.

Figure 3-1 Activity monitoring software allows employers to watch employee computing activities.

Using the Internet to Build a Good Reputation

Point out to your students that it is possible to use online sites to build a great online reputation. Just as a great resume presents you to the working world, responsible and ethical online behavior can help a student get into a school or land a dream job. Creating a terrific online image can be a positive thing if the motivation is not to deceive, but to put your best foot forward.

If your students are older and beginning to think about launching their careers, encourage them to contribute to sites that relate to their field of study or career goals, whether in discussion forums or by replying to blog comments.

These materials are the copyright of Wiley Publishing, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.
posts. This helps to establish their interest and knowledge in particular subjects. Also, career networking sites, such as LinkedIn, help them to connect with others in their chosen fields.

Finally, students should consider launching their own Web sites that they can do for free using services, such as OfficeLive. They can use those Web sites as online portfolios for writing or artwork or to connect with those with similar interests.

Suggest that students reach out to professionals online to advise them about career directions or to act as a thesis consultant. They may be surprised by how many folks who write books or run Web sites are happy to help younger people get off on the right foot, and the Internet is an easy way to connect with them.
Chapter 4
GETTING A HANDLE ON CYBERBULLYING

Chapter Check-in

❑ Cyberbullying is relentless
❑ The issue permeates the classroom and schools are being required to address it
❑ Victims lack self-esteem and friends and are natural targets, but are not at fault
❑ Bullies typically suffer in later life from substance abuse, and failing at jobs and relationships
❑ Build a climate of zero tolerance for cyberbullying in your school

Many of you have read the headlines of the tales of teens or tweens who have harassed others using instant messaging, texting, and social networking blogs to the point where the victim commits suicide. So, what exactly is cyberbullying?

Cyberbullying is plain old bullying transformed into a much worse problem by the coming of the digital age. It can consist of

■ Use of cellphones, e-mail, or instant messaging to send a barrage of harassing messages to a victim.

■ Use of cellphone cameras to take embarrassing photos and then passing them around the Internet.

■ Use of phony personas or Web sites to upset or shame a victim or spread lies. Some cyberbullies create Web sites and pretend to be the victim to alienate him or her from friends.
The main difference between schoolyard bullying and cyberbullying is that it occurs 24 hours a day, 7 days a week, and can expose a victim to ridicule and embarrassment not in front of a few classmates, but in front of the entire world.

Why Is Cyberbullying a School Issue?

Some people have stated that they feel schools should not get involved in cyberbullying situations. But why shouldn’t schools be involved when the reality is that cyberbullying goes on throughout the school day, so schools are not bullying free zones? In addition, the classroom environment is affected by a climate of cyberbullying. When cyberbullying ends in a student suicide or beating, schools must deal with the shock and pain within their walls in reaction to it.

Many states are now mandating cyberbullying curriculum and more school districts are scrambling to find or create curriculum materials. In Figure 4-1, you see an example of one program a school instituted to address cyberbullying.

Figure 4-1 This school district offers useful links to learn about cyberbullying.

Cyberbullying varies by grade level. Young children do not seem to get into this behavior, in part because they have less access to personal computing devices. High schoolers generally have outgrown their cyberbullying tendencies, but it is still possible. Middleschoolers tend to test limits.
and obtain their first cellphone and cyberbullying hits a peak. In addition, girls tend to cyberbully more than boys.

If you are interested in the variety of material on cyberbullying available, check out these resources:

- Search YouTube for some excellent Ad Council videos on cyberbullying.
- Stopcyberbullying.org is a Web site with a program produced by WiredSafety that provides information broken into three age levels.
- Seattle Public Schools cyberbullying curriculum is free at www.seattleschools.org/area/prevention/cbms.html.

**How Does Cyberbullying Hurt Victims?**

Victims of cyberbullying feel that there is something about them that caused the bullying. They are too tall or fat, their ethnicity or religion is at fault, they have dated the wrong people. The reality is that most bullies choose a victim—somebody who has few friends and lacks self-esteem—and then finds a focus for the bullying.

Beyond the humiliation, victims of bullying live in fear. In the United States every day hundreds of thousands of kids stay home because of the fear of bullying. However, in this digital age, staying home is no longer the answer because bullies have long digital arms that follow victims everywhere.

Tragically, some cyberbullying victims end their lives because they can’t live with the constant nature of the attacks and the public nature of the humiliation when damaging information or pictures are posted online.

Important signs to look for in someone you think is being bullied include the following:

- A reluctance to go to school
- Tiredness caused by middle-of-the night contacts
- A lack of self-esteem

Victims may also break off friendships, a result of a bully’s tactic of isolating targets and attacking them while pretending to be their friends.

These materials are the copyright of Wiley Publishing, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.
How Does Cyberbullying Hurt Bullies?

Though we feel for victims of bullying, the reality is that the bullies themselves may suffer more in the long run. Studies have shown that those who bully in school are often headed for a life that may include prison, dead-end jobs, alcoholism, or drug abuse. Bullies also find it hard to make and maintain relationships.

Because bullies find that aggression is an easy path to getting what they want, they never learn other coping tactics, such as compromise and negotiation. They are therefore unpopular at work and in relationships. Turning around these behaviors and attitudes before students leave high school is vital to helping them succeed in later life.

Bullies are often the product of a bullying environment at home. They have learned this behavior from one or more parent and need examples of other ways to behave to get what they need in life. As a teacher, there is not a lot that you can do legally to get involved, but as that school mentor, try to help students learn to negotiate and compromise in classroom settings.

How to Deal with a Cyberbullying Situation

If you have noticed that your students are acting different and your suspect cyberbullying or if students have come to you and told you that cyberbullying has occurred, you must act. Preventing and coping with cyberbullying in your school is important, and here are some helpful tips:

- The best way to deal with cyberbullying in a school is to create a climate where cyberbullying (or any kind of bullying) is not tolerated and not cool. Set clear rules about cyberbullying and enforce them.

- Run an educational campaign to help kids understand why they shouldn’t bully and the consequences of becoming a bully. Use Web sites, such as Stopcyberbullying.org (see Figure 4-2) to help you plan the campaign.
Figure 4-2  Stopcyberbullying.org from WiredSafety.

- Bullies go after people with no support system. If students stand by a victim, often a bully backs down.
- Create a bullying policy and enforce it.
- Help everybody understand that the victim is never at fault. A victim does not bring bullying on himself and should not be made to feel guilty, which only aggravates the pressure on that person.

Cutting kids off from the Internet and their cellphones are not the answers. That “solution” further isolates them and removes an essential part of their lives. Instead, parents may consider taking a cellphone when their child goes to bed so calls aren’t arriving in the middle of the night. Encourage victims to make their own social networking pages private so bullies can’t post comments or gather information about the person to use as ammunition.
Chapter 5

TEN GREAT ONLINE SAFETY WEB SITES

Chapter Check-in

❑ Discovering vital tools for safety
❑ Using the Internet to protect students from the Internet

Many online safety sites out there offer information, online tools, videos, podcasts, and more to help you learn about and teach online safety to students. This chapter gives you the top ten recommendations.

iLookBothWays.com

This site is run by the LookBothWays educational foundation, which is leading the effort to develop a comprehensive online safety curriculum that is free to all schools. Founder and internationally known expert Linda Criddle was the MSN child safety expert at Microsoft for many years and you can ask questions of her as well as access informative articles and online safety tools here.

SafeInternet.org

This Web site is the site of the Safe Internet Alliance, a consortium of technology industry companies concerned with online safety issues. This source is a great place to get information about current news and legislation related to online safety, as well as information about online safety-related events.

These materials are the copyright of Wiley Publishing, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.
WiredSafety.org

WiredSafety.org was created by lawyer and Internet safety advocate Parry Aftab. The site offers a free Stop Cyberbullying toolkit and is a great resource on Cyberlaw issues, such as free speech and privacy. The site’s Tweenangels and Teenangels programs run a WiredKids Summit every year presenting results of research that the kids have performed to adults.

InternetSafetyEducator.com

Check out this site for a good source for Internet safety news and information about safety legislation. You can also find teacher resources for online safety curriculum, online worksheets, lessons, and more. Use this site too to find online games for younger kids to use in a safe environment to help them learn using technology.

SafeKids.com

This UK-based site covers news about online safety. It’s a good way to get a more international perspective on the problem because issues do tend to differ a bit from country to country. Assigning your kids to research a topic on this site may bring in some new perspectives on the global Internet.

Coolcatteacher.blogspot.com/index.html

Teacher and online safety advocate, Vicky Davis, runs this site. This blog offers updates on online safety news and great tips about how teachers can use technology in the classroom in a positive and safe manner. She also offers lesson plans related to use of technology in the classroom.

FBI Parents Guide

This site, FBI.gov/publications/pguide/pguidee.htm, offers advice about what to do if a child is a victim of online abuse, sexual predation, or cyberbullying. Especially useful is information on how to spot signs of such abuse and how to report such abuse to law enforcement.
**Netsmartz.org and Netsmartzkids.org**

These sites, sponsored by the National Center for Missing and Exploited Children, have useful content addressing younger kids, parents, teens, educators, and law enforcement. The source includes fun, animated games, videos, and activities that are especially useful with younger kids.

**iKeepSafe.org**

This organization was started by the Internet Keep Safe Coalition, a partnership of governors and first-spouses, as well as attorneys general, industry, and law enforcement professionals. You can join their educators group for access to educational resources.

**CommonSenseMedia.org/educators**

This site supports responsible use of media by kids. They have some excellent resources for educators, including an educator’s kit, educator discussions, school surveys, and school discussion guides.
Chapter 6

TEN TIPS FOR CREATING STRONG PASSWORDS

Chapter Check-in

❑ Discovering the tricks of the trade
❑ Protecting yourself and students from hackers

Strong passwords and pass phrases are vital to preventing unwanted access to online accounts, from social networking sites to financial institutions and online stores where a credit card number is stored for making purchases. Many people are intimidated by creating strong passwords because the passwords seem difficult to come up with and less easy to remember. However, learning a few simple rules and tricks makes it simpler.

Make It Longer

 Longer passwords are harder to figure out. Try for about 10 characters minimum. Some sites require that you have a minimum number of characters for your password, which is a good practice on the sites’ parts. Other sites don’t let you use more than 6 or 8 characters, for example. Just make the password as long as possible given the parameters.

Use Variety

Most people know that mixing up letters, numbers, and symbols, such as $!@, makes a stronger password. Again, some sites require a mixture of characters while others won’t allow symbols. You can also use a combination of uppercase and lowercase letters to make stronger passwords, if a site doesn’t allow symbols. To help you remember such a password, try...
using a pattern from your keyboard, for example starting at the top left corner and forming a “W” pattern, a very strong and easy to remember password would be lqSXdr5ThnJi(.

**Don’t Include Personally Identifiable Information**

Putting personally identifiable information in a password is asking for trouble. This information may include your name, street name, child’s name, or car model. Anything that is a matter of public record, such as your birth date or address is easy for a crook to find out. Instead, use a favorite song or literary phrase (perhaps with some numbers and symbols mixed in, such as 2BorNo+2Be).

As an in-class exercise, have students create strong passwords that include no personally identifiable information. Make sure they don’t use any actual passwords they use online!

**Avoid Repeated Letters or Numbers**

Hackers can use programs to find instances of numbers in your password. If your password is 555John777, when the program finds 5 and 7, it’s scored six hits instead of two. Time is often of the essence for those trying to break passwords—because they can only do two or three tries before being locked out of an account. Don’t make it faster and therefore easier for hackers to break your password.

**Avoid Common Words**

A dictionary attack is a technique that uses a program to scan through all the common dictionary words in trying to break your password. Dictionary attacks can go through thousands of words in minutes. If your password is Airplane7, the word portion of the password will be found in seconds, which leaves only 9 numbers to run through to guess the entire password.

**Spell Words Backwards**

If you want to use a common word, spell it backwards and mix it up with numbers and symbols. For example, you might make your First National Bank account password “lano1tNKna8,” with the 1 and 8 standing in for the I and B.

These materials are the copyright of Wiley Publishing, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.
Keep Passwords in a Safe Place

Everybody advises you not to write down passwords, but that’s not a very practical suggestion. It’s okay to write them down, but just don’t keep the list near your computer and don’t leave it where others can easily find it. Also, don’t ever share passwords with others; today’s friend can become tomorrow’s enemy.

Change Pass Phrases Often

One of the best defenses to having your accounts hacked is to change your passwords regularly—say every couple of months. This practice is especially important on any financial account or retail site that has your credit card on record for purchases.

Don’t Use the Same Password Everywhere

You should never use the same password on multiple accounts, because once that password is broken, it opens the door to all your accounts for a clever thief or bully.

Be Cautious about Password Hints

In addition to strong passwords, you should be sure to take care when creating password hints because thieves may use the “Forgot your password?” feature on many accounts to reset the password and access your account. Typical password hints are mother’s maiden name, high school attended, and so on. The problem with those is that they involve publicly available information. If you are limited to preset questions and they are of this type, you have the option of using a false answer. The company doesn’t care what you answer as long as you match that answer every time you use the feature. If your mother’s maiden name was Smith enter Jones. If you can choose among a broader range of questions or create your own, choose one that involves non-publicly available information, such as your favorite movie or the place you first met your partner.
Chapter 7
TEN GUIDELINES FOR SAFER BUYING AND SELLING ONLINE

Chapter Check-in

❑ Making safe purchases online
❑ Reducing your risk of financial ruin

You can come across several types of buying and selling experiences online, from buying at a well-known retail site, such as Amazon.com, to selling your treasures on an auction site or buying or selling on an online classified site. Each can carry certain risks. Your students are probably already buying ringtones and apps (applications) for their cellphones, unless they are very young. Some may even have accounts at online stores. But eventually, all of them will be online shoppers, so now is the time to instill some common sense advice about buying and selling online.

Choose the Best Payment Method

You can pay for services and goods online today with many different types of payment. Some are good and some are not. The very best method to use for online payments between individuals is a payment service, such as PayPal. These services hold the funds until a buyer releases them, acknowledging that the item was received in good condition. These services also offer conflict resolution support in case there is a problem with the sale.

Some of the not-so-great ways to pay include the following:

■ **Check**: You should *never* pay with a check for an item you buy from an individual (or even a small business) on a classified or auction site. This practice puts your checking account number in a stranger’s hands.

These materials are the copyright of Wiley Publishing, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.
Credit card: Credit cards are typically protected from fraud leaving you at risk for only about $50 of any illegitimate charge you can’t reverse, so they aren’t a bad option. Still, giving your credit card number to a stranger is a bit risky. If that person abuses the number, you’ll have to cancel the card and have another one issued.

Use Stores You Know

If you have dealt with the company in the ‘brick and mortar’ offline world and found the company reputable, you’re probably fine shopping at their online site. Things to be alert for here include the quality of their customer support and their shipping and refund policies. Perfectly reputable businesses may limit returns to a 14-day window and charge a restocking fee for certain types of merchandise, for example.

Identify Trusted Online Sites

If you choose to shop on an online retail site, the most important thing is to identify trusted sites. If you’ve never shopped at an online store before, you should do your homework.

Check for customer reviews of the business at sites, such as

- www.Epinions.com to see what experiences others have had
- The Better Business Bureau at www.bbb.org—search for ratings for any business
- McAfee Site Advisor installed on your computer—performing a search with this type of product will flag sites that tend to download malware to your computer

Deal Locally with Classified Ads

Classified ad services, such as Craig’s List, were started with the idea of locals connecting with each other to buy and sell items. Of course, those ads are available to people around the world through the Internet, but you should know that the risk of fraud increases exponentially if you deal with somebody who doesn’t live in your area. You should always avoid

These materials are the copyright of Wiley Publishing, Inc. and any dissemination, distribution, or unauthorized use is strictly prohibited.
exposing too much personal information in your listing (your location or phone number, for example). Be wary of people who try to get items for free with hard-luck stories or who offer to pay more than the price you stated. These are invariably signs of a scam.

**Use Sites with Secure Transaction Technology**

When you are on a page that is part of the purchasing process, make sure that the site address in the address bar of your browser begins with **https** instead of http. This small difference tells you that there is a technology being used to protect transmission of your credit card or other financial data during the purchase from hackers.

**Don’t Let People Come to Your Home**

If you sell an item through an auction or classified ad site, avoid having buyers come to your home. If an item is portable meet the person in a public place. If it is not portable, be sure somebody else is with you when the person visits.

**Don’t Hand-Out Your Password**

Having accounts at online retail sites that store your credit card is fine because your cards are protected from fraud. However, having that payment information on record could cause some headaches if somebody else accesses your account, including the time and effort you need to straighten out a phony transaction. An account number at a retail store can be like a blank check to those who want to take advantage of you. Protect your online account information as you would the passwords to a bank account.

**Use the Protection of the Auction Site**

Sometimes when you post an item in an auction site for sale individuals will contact you via the site’s e-mail setup and ask to speak to you in person or e-mail to your personal account. Often these people will ask if they can purchase the item outside of the auction site. It’s always better to transact business under the protection of the auction site, which has policies for behavior and payment systems that can help keep you safe.
Delete Your Personal Information

If you sell an electronic item, such as a computer or cellphone online, be sure that you erase all personal information from it. This information may include contacts, stored passwords in your browser used to access online sites, financial records in spreadsheet or banking applications, tax records, and so on. Kids get into selling these hi-tech devices online so they can buy new ones on a frequent basis, so this piece of advice is important for your middle-school and high school students.

Watch Your Costs

Kids are getting cellphones at a younger age these days. Cellphones provide a great way to stay in touch or call for a ride or ask for help if a problem arises. However, they also provide a way to rack up costs if a child downloads ringtones, graphics, and applications. Even at $1.99 apiece, these purchases, typically applied to the parents’ phone bill, can add up. Advise students to be prudent about these small but potentially pricey purchases.
Inside, you find out …

- How to talk to kids about online safety
- How to avoid personal information exposure
- How to educate students on cyberbullying
- What types of activities you can use with your students

Nancy Muir has taught Internet safety courses at two major universities and runs a Web site on seniors and computing (techsmartsenior.com). She is the author of over 60 books on technology topics and a Vice President at LookBothWays—a company specializing in Internet safety education. Nancy also writes a regular column on computers and the Internet at Retirenet.com.

Visit us online at CliffsNotes.com®