make the best of your online adventures

jo cool

jo fool

at

www.media-awareness.ca/english/special_initiatives/games/joecool_joefool/index.cfm

Teacher's Guide

Table of Contents

The Jo Cool or Jo Fool online module is followed by a quiz comprising of twenty questions that address the issues that students have explored through Joseph and Josie's online adventures.

Students can complete this quiz online at:
www.media-awareness.ca/english/special_initiatives/games/joecool_joefool/index.cfm

Introduction

Welcome to the Teacher's Guide for Jo Cool or Jo Fool, a tongue-in-cheek online module where students rate the decisions made by the brother and sister team of Joseph and Josie Cool as they encounter opportunities online, and learn a bit about safe and savvy surfing in the process.

The Jo's adventures on the Net, which can be found on the Media Awareness Network Web site at <www.media-awareness.ca/english/special_initiatives/games/joecool_joefool/index.cfm>, are based on real online experiences encountered by kids and teens. Each scenario represents specific issues and challenges that kids face when they surf the World Wide Web. The situations are intended as springboards to help kids surf wisely and begin to think critically about online privacy, online marketing, responsible Internet use, authenticating online resources and Internet safety.

As kids visit each of Joseph and Josie's bookmarked Web sites, they are asked whether the Jo's are making wise decisions. Students can write answers in media journals and compare them with classmates after viewing each of the Web scenarios, or when the entire module has been completed. Key questions to consider are:

- *What kind of Web site is this? What is its purpose: To inform? To sell? To entertain? To persuade?*

- *Is it a commercial Web site? A personal home page? An educational site? How can students tell?*

- *What decision does Jo have to make?*

- *What should Jo look out for? What should he or she take into account before acting?*

- *What's the "big picture" here? Is this a privacy or safety issue? A matter of authentication? Does this relate to good citizenship online?*

- *Does Jo make the right decision? Why or why not?*

In this guide, Joseph and Josie's scenarios have been categorized according to the Internet issues they raise. Each Internet issue section contains background information on the issue; links to summaries, questions and activities for related Jo Cool online scenarios; and links to additional resources on the Media Awareness Network Web site.

The *Jo Cool or Jo Fool* module is followed by an online multiple-choice quiz that reinforces the lessons that have been learned. A summary of questions and answers is included in this guide.

Online Marketing to Kids and Privacy Issues

The Internet is a marketer's dream – especially when it comes to reaching young people. Kids today have tremendous buying power; and with the Internet fast becoming an integral part of kid-culture, it's not surprising that marketers are looking for ways to capitalize on this engaging and powerful medium.

- **Canadian 'tweens (ages 9-14) have $1.8 billion in total discretionary income, and influence ten times that amount in family spending.** *Source: YTV Kid & Tween Survey, September 2000.*

- **Coincidentally, by 2006, it's estimated that Canadian kids and teens will spend $1.8 billion dollars online annually.** *Source: Forrester Research, 2001*

The Internet's interactive nature permits companies to create online environments where advertising is seamlessly integrated with graphics, games and activities. These virtual playgrounds aim to foster brand recognition and brand loyalty.

Marketers also capitalize on the Internet's potential for collecting personal data from young people. They do this through the use of online registration forms which kids must complete to become members of Web sites, play games, collect prizes or participate in activities. The collection of personal information through online quizzes and surveys is also quite common.

In the United States, legislation restricts the gathering of information from children under the age of thirteen. Problems arise when kids under the age of thirteen visit Web sites aimed at older teens – sites that don't have to adhere to these regulations. Collected information may be sold to other companies, used for market research, or used to create extensive customer profiles. All collected information is intended to improve a Web site's ability to reach its target audience.

It's important for young people to understand that although commercial sites are fun, they are also big business. Kids should recognize when, and how, they are being sold to. Educators can help kids understand the role advertisers play as creators of Internet content by teaching them to deconstruct the online marketing techniques they encounter.

A greater challenge is persuading kids to value their own personal information. Studies suggest that young people have little concern about their privacy on commercial Web sites – especially if there's a chance they might win a prize. The Media Awareness Network's survey *Young Canadians in a Wired World* found that over 50 per cent of Canadian kids will reveal their gender, age, hobbies, name and e-mail address in order to win a contest.

Should we be concerned? In her article *Capturing the "Eyeballs" and "E-wallets" of Captive Kids in School,* Internet ethics expert Nancy Willard observes:

> **Dot.com companies are asking children to disclose personal information and then using that information to develop a close relationship with the child for the purpose of influencing consumer behavior. Such companies are working with child psychologists to gain better insight into the thinking of children to improve their ability to manipulate the child for commercial purposes. This is commercial exploitation. But the potential of injury to children from this kind of exploitation may be greater than simply damage to the pocketbook of the child or parent. Children raised in such an environment will likely fail to develop an understanding of the appropriate boundaries of personal privacy. They will be extremely vulnerable to all manner of manipulation and exploitation, not only from corporate marketers, but also from scam artists, cults, and sexual predators.**
>
> **http://netizen.uoregon.edu/documents/eyeballs.html, page 10.**

Helping kids to understand that they and their personal information are viewed by marketers as commodities is an important first step in creating informed consumers.

_____

Jo Cool Scenarios for Online Marketing and Privacy

The following scenarios address online marketing and privacy: Lotsa Music (page 8), Splurge Cola (page 6), and CD-Rama (page 10).

Additional Resources

Background materials for teachers:
- MNet's Kids for Sale section contains many resources on online marketing and privacy.
- For teachers who want to delve into this topic in more depth, MNet offers the Web Awareness workshop for professional development: Kids for Sale: Online Marketing to Kids and Privacy Issues. (Both these resources can be found in the Web Awareness Section for Teachers.)
- The Center for Media Education reports: Web of Deception: Threats to Children from Online Marketing <www.cme.org/children/marketing/deception.pdf>and And Now a Web From Our Sponsor: How Online Advertisers Are Cashing In On Children <www.cme.org/publications/infoactive_files/22/22nweb.html>.
- Industry Canada has created a guide to shopping on the Internet that includes a handy tip-sheet for consumers called, Internet Shopping Tips <http://strategis.ic.gc.ca/SSG/ca01184e.html>.
- The American Federal Trade Commission <www.ftc.gov/bcp/menu-internet.htm> offers an e-commerce page for consumers that includes tip sheets on a wide assortment of consumer-related Internet issues.

Lessons – access the following lessons using the Media Awareness Network's search engine:

Online Marketing to Kids
This lesson introduces students to the online marketing techniques used to target children on the Internet, and helps them to understand the similarities and differences between traditional marketing methods and online advertising.

Protecting Your Privacy
In this lesson, students explore the ways in which commercial Web sites collect personal information from kids, as well as the issues surrounding children and privacy on the Internet.

Online Marketing Scenarios

Splurge Cola

When Josie visits *Planet Splurge*, she has to sign up in order to participate in the many fun-sounding activities on this Web site. The registration form asks her for her name, age, gender, address, phone number, favourite band, favourite food and future career plans. She's also invited to submit the e-mail addresses of several friends, who will receive *Splurge* e-cards on her behalf.
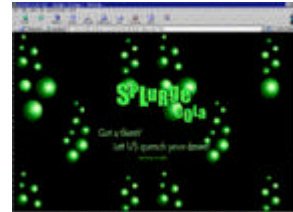
What kind of Web site is this?

Like *Lotsa Music*, this is a branded commercial Web site that Jo feels comfortable in because she enjoys drinking *Splurge* cola.

What decision does Jo have to make?

Jo has to decide whether it's worth submitting personal information in order to participate in the site's activities.

What should Jo look out for?

Often there's quite a discrepancy between the "all in fun" language on a Web site and the underlying legal language. The *Splurge Cola* site is big on hype and works hard to appeal to teens. However, it's important that Jo check out the legal fine print before she joins. Jo's first stop should be *Splurge Cola's* Privacy Policy.

Jo should also take note of the marketing strategies on the *Splurge* site and recognize that there are probably commercial connections between the company that owns *Splurge Cola* and the products and artists featured on the site. Many Web sites offer advertisements, brand-related prizes, gimmicks, games and activities in exchange for advertising dollars. This doesn't mean that kids can't visit and enjoy commercial environments – but they should understand that commercial Web sites are marketing vehicles.

Does Jo make the right decision? Why or why not?

Jo has some things to learn about protecting her privacy online. She's not only a potential marketing target for *Splurge* – her personal information is also a commodity that can be sold to third parties. Before Jo provides any information to *Splurge*, she should be sure that her personal information won't be sold or distributed to other companies; what information is being collected or tracked, and how it will be used; how she can change or delete any information she doesn't want *Splurge* to have; and which companies are behind the *Splurge Cola* site.

Jo should also take *Splurge's* hype with a grain of salt, and recognize that this company probably has a vested interest in the bands and products promoted on its Web site. As well, Jo should recognize the "Spread the *Splurge*" e-card promotion for what it is: a marketing ploy to bring new customers to the site.

Additional Questions to Ask Students

- Do you think it would be appropriate for Jo to use false information to register for the *Splurge* site? Why or why not?

- What's your opinion of gimmicks such as e-cards? Would you mind receiving one? Would you mind a friend submitting your e-mail address to a company without your permission?

- What do you like most about commercial Web sites?

- What do you like least about them?

- Have you ever filled out a registration form to participate in an activity on a Web site?

- If so, were you contacted by the Web site? How often?

Online Marketing Scenarios

Lotsa Music

Lotsa Music is the official Web site for a popular rock video TV show. When Joeseph visits the site, he has the opportunity to enter a contest and win a prize.

In order to enter, Jo must submit his first and last name, age, home address, phone number and e-mail address – along with his answer to the trivia question.
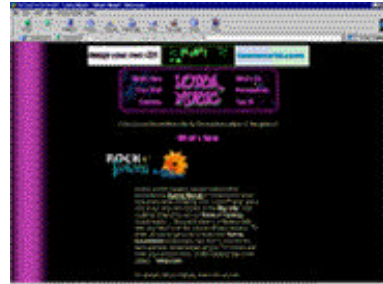
What kind of Web site is this?

Jo's visiting a branded commercial Web site. He's comfortable with *Lotsa Music* because he's a regular viewer of the television program.

What decision does Jo have to make?

Jo has to decide whether or not to enter an online contest that requires him to submit personal information. Because Jo is a fan of the television series, and knows the answer to the trivia question, he sees nothing wrong with entering the contest.

What should Jo look out for?

Before Jo enters an online contest, he should take the time to read the contest rules and regulations in order to ensure that any personal information he submits to the Web site is secure.

Does Jo make the right decision? Why or why not?

Jo made the wrong decision because he didn't take the time to check out the rules and regulations for this contest. As a result, Sunny Musak has his personal information and is free to use it in any way it sees fit – whether Jo wins the contest or not. Jo's personal information can be sold to other companies, used in advertisements or posted on affiliated Web sites all without compensation.

This sort of release is fairly standard for most contests. But the ease with which kids can submit information online doesn't encourage critical thinking. Young people should always understand the terms and conditions of any contests they enter – online or off.

Additional Questions to Ask Students

- Have you ever entered a contest on the Internet?

- If so, did you have to submit any information? What was it?

- Were the contest rules easy to find?

- Did you read the contest rules?

- Were the rules clear and easy to understand?

- Did the rules say what would happen to any information you submitted?

- Do you feel that corporations like Sunny Musak have the right to ask for this information?

- Do you feel comfortable submitting your personal information to such corporations?

- How is entering a contest on a Web site different from entering a contest by mail? How is it similar?

Extension Activity

- If your classroom has computer access, go online and have students read the rules and regulations for a few online contests. (Web sites for snack foods and soft drinks are usually a good bet for these activities.) Have students note the layout of these rules and regulations, often they only appear in small print, in a small window, after much scrolling. Does this layout encourage or discourage close scrutiny?

Online Marketing Scenarios

CD Rama

CD Rama is an online music store where customers can purchase CDs from a wide range of artists. It even permits visitors to create their own CDs by combining music files from *CD Rama's* archives. This site appears to be respectable: it uses encryption software, protects personal information, and is certified by the Better Business Bureau.

What kind of Web site is this?

CD Rama is a commercial Web site that makes its money selling custom CDs.

What decision does Jo have to make?

Jo has to decide whether it's safe for him to purchase CDs online from *CD Rama*.

What should Jo look out for?

Jo should look for indicators that this Web site is secure and reputable. Is the company well-known? Does it have a good reputation? Does it offer consumer protection? Does it respect personal information? Does it have a secure transaction system? Does it clearly state purchasing terms and conditions? These are all questions Jo should ask.

Does Jo make the right decision? Why or why not?

Jo has done his homework on this Web site. He knows he will get a quality product because he has made sure that *CD Rama* is a reputable merchant. This ensures that his transactions are protected.

Additional Questions and Activities

- Many Web sites encourage visitors to pay for goods directly, online. What are some ways to tell whether it's safe to give a Web site your credit information? (Answers may include: checking for quality assurance certificates or seals; clicking on the padlock icon in the bottom corner of the screen – a "https" notation appears in the URL when you are on a secure Web page; checking out the safeguards that protect payment information you submit; and reading the site's policies on collection and distribution of personal information.)

- Just because your payment is protected, that doesn't mean that you're going to be happy with your online purchase. What other questions should you ask? What's the full cost of this product, including shipping and taxes? Are there any limitations or restrictions on the sale? Can I cancel the order if I change my mind? What about warranties and guarantees? Can I return it if I'm not satisfied? How do I return it?

- *CD Rama* customers can both purchase CDs created by a particular recording artist, or they can create their own CDs that include music produced by different artists. *CD Rama* pays royalties to the record companies each time a CD or piece of music is sold, much like a music store in the real world. There has been a lot of debate about the sharing of music files using software like Napster. This software permits people to exchange music files for free, without paying royalties to recording companies or recording artists. The issues at the heart of the Napster debate are worth exploring and discussing in the classroom. A search for Napster at <www.britannica.com> will bring up information on all sides of this controversy. Students might like to present their findings from various perspectives: Napster, Internet users, the recording industry, and recording artists.

> **Did You Know?**
>
> **According to Canadian copyright law, Napster might not be considered illegal in Canada. In Canadian courts, Napster would probably have to change the way it presently operates – but it wouldn't have the problems it has experienced in the United States. This is because:**
>
> **"The Canadian Copyright Act exempts intermediaries from copyright liability provided that they function strictly as a conduit in the transfer of data."**
>
> **This means that as long as Napster only functions as an Internet Service Provider that permits people to share files – and doesn't post, modify or block content, or actively encourage its users to violate copyright law – then it is operating within the Canadian Copyright Act.**
>
> **Canadian copyright law states that users of Napster aren't breaking the law as long as:**
>
> **They only copy sound recordings of musical works for their own private use and do not post this music online for others to download.**
>
> **Also, unlike the United States, Canada charges a tax on all blank audiotapes and CDs. This money is then returned to the recording industry to compensate for lost revenues. (A contentious issue in the United States is compensation for the recording industry, which claims it is losing millions of dollars in revenue.)**
>
> **Source: Globe and Mail, July 27, 2000**

For an in-depth comparison of Canadian and American laws pertaining to online file-sharing, read David Ullman's "Napster and Beyond: Copyright Issues and Solutions"
<www.mggg.com/publications/napster_and_beyond_copyright_issues_and_solutions.pdf>

- Compare Canadian copyright law to American copyright law. Can you think of other online activities these laws might apply to? (For instance, swapping movies online will soon be as commonplace as swapping music. How will the motion picture industry deal with this?)

- How is this issue a good case study for the problems of regulating the Internet? If Napster were based in Canada, could the United States do anything to stop it?

- Research what is presently happening in Canadian and/or U.S. courts on the issue of using online file sharing software to exchange music or movies.

Extension Activity

Visit a few retail Web sites and check out any consumer protection features.

Online Safety

Most young people who go online have positive experiences, but there are some drawbacks and safety issues that adults need to be aware of. In order to maximize the Web's positive aspects, we need to identify and respond to online environments and activities that can put kids at risk. Those risks may include exposure to pornography and other sexually explicit material; violent, dangerous or illegal information; promotion of unhealthy or antisocial activities; and compromised personal privacy in interactive activities such as chat, e-mail and Instant Messaging.

According to the Media Awareness Network survey, *Young Canadians in a Wired World*, Canadian kids and teens have much to learn about staying safe online.

- **More than half the 13-14-year-old Internet users surveyed visit private and age-inappropriate chat rooms.**

- **Nearly three out of ten children and teens who use the Internet have been asked for an in-person meeting by someone they've only met on the Internet.**

- **Sixteen per cent of children and youth who have used the Internet have actually met someone in person they had only previously talked with on the Internet.**

- **Boys are more likely than girls to go alone to meet Internet acquaintances in person.**

- **More than half the kids who use the Internet have accidentally ended up in a pornographic Web site.**

- **Children who encounter negative experiences online are most likely to rely on friends or their own ingenuity to deal with the situation.**

- **Almost one-half the kids in secondary school say that someone has made unwanted sexual comments to them on the Internet.**

- **Some 25 per cent of Internet connected kids have their own personal Web sites. Of these, almost six in ten say they post their e-mail address on their sites.**

In order to help young people avoid risky online situations, it's important that educators take a measured and balanced approach to the Internet – considering both its pitfalls and its advantages, since online experiences can be useful and positive. Knowing what kids do on the Internet is a good start. Where do they go online, and what are their favourite activities? What are the benefits and the risks associated with these activities? And finally, how we can minimize the risks and maximize the Internet's potential as a fun, positive place for kids?

Kids aged 11-13 are very likely to test ideas and online experiences that are outside their "real world" boundaries. They also experiment with alternative identities or behaviour. Yet these kids are less likely than their younger siblings to be supervised while they surf. This group sees the Net and computers as "cool", and their natural affinity for socializing means that they enthusiastically participate in interactive activities such as e-mail, Instant Messaging and chat.

Kids in this age range usually integrate themselves into self-selected Internet communities. The importance of chatting increases, and the Internet becomes a way to meet new people they would never encounter in "real life," and to establish relationships with them. To these kids, the Internet is a place to go to. They take the Microsoft slogan "Where do you want to go today?" very literally.

The freedom to experiment with online personas and build online communities can be an empowering experience, especially for children with disabilities or low self-esteem; but there is a downside to the Net's anonymous nature. Although many adolescents are savvy about "stranger danger" in the real world, these skills may not work in the world of cyberspace. While kids seem to understand that giving out private information to strangers isn't a good idea, their definition of "strangers" may not include corporations whose logos or brands they recognize – especially if there's a chance they might win a prize by entering a contest. Many young people give little thought to what will be done with their personal information once it's collected or who will be able to access this information if it's posted online.

Young people's definition of "stranger" may also not apply to people they correspond with online. Friendships can grow quickly on the Internet, and this can lead to problems. Preliminary focus testing for MNet's kids' survey found that although girls in the 11-14 age range would initially omit or protect information about themselves in chat rooms, they found it impossible to do so after a certain length of time – which ranged from several weeks to 15 minutes.

A word about filtering...

- **In response to safety concerns, many parents and educators are turning to technological tools as a means of protecting young people. Filters and blockers do have their place, especially for young children. But filtering can be problematic.**

- **First, filters don't filter perfectly – they can still let in information you don't want and may also prevent students from accessing valuable information. The American Library Association says that filters fail to block out about 15 per cent of sites containing objectionable content and as much as 20 per cent of appropriate sites that would be useful.**

- **A second downside is that using technology to block kids' access to information can actually motivate kids to get to that information, at school or at home. It's the old "forbidden fruit" syndrome.**

- **Most importantly, though, kids should learn to live in the real world – which today includes the virtual world. If we keep them in cyber-bubbles as they grow up, they won't acquire the skills they need.**

- **Certainly, very young children (age 5-11) should be protected. They need close supervision, some good rules – and some early training in critical thinking. But once they get to high school, students need a great deal of training in critical thinking, a good deal of information, and much less protection.**

To maximize the positive aspects of online interactivity and community-building, teachers can provide students with safe, moderated interactive environments. At the same time, students need to understand:

- the importance of safeguarding their personal information in chat environments and on Web pages

- how to recognize when they are being targeted online, and how to avoid it

- what to do if they encounter an online situation that makes them feel uncomfortable or scared

- how to recognize safe Web environments

- how to conduct effective Web searches that minimize exposure to inappropriate materials

The only real protection we can give young people is a practical set of the critical thinking skills they will need for the Internet – as both it and they grow and develops. Adults who are familiar with Web environments and activities are better able to guide and discuss the online explorations of young people. For educators who aren't familiar with the Internet, a good start is to let students provide a tour of the Web sites and activities they enjoy. The Safe Passage section of Web Awareness for Teachers offers background information on Web sites, newsgroups, chat rooms, Instant Messaging and e-mail. *Safe Passage* also explains how these environments work, what value they offer, what risks they may pose for young people, and what teachers can do to minimize those risks.

Jo Cool Scenarios for Online Safety

The following scenarios – Jo's Home Page (page 18), and Fast Talk (page 15), address the issue of online safety.

Additional Resources

Background materials for teachers:

MNet's Safe Passage section contains many resources on this topic, including:

- General Internet Guidelines for the classroom
- A series of case studies for classroom discussion
- Information on protecting children from online predators

For teachers who want to delve into online safety in more depth, the Web Awareness section for teachers features the professional development workshop: Safe Passage: Teaching Kids to be Safe and Responsible Online.

Handouts – access the following handouts using the Media Awareness Network's search engine:

- Internet Checklist for Kids, ages 9-12
- Internet Checklist for Teens, ages 13-17

Online Safety Scenarios

Fast Talk

According to surveys, chatting is one of the most popular online activities for teenagers. Josie's brother, Joseph, met his girlfriend online, so Jo hopes she too will be able to find the boy of her cyberdreams in one of *Fast Talk's* many chat areas.

What kind of Web site is this?

Fast Talk is an unmonitored online chat environment for teenagers and young adults. It offers a series of chat areas on several topics – including dating.

What decision does Jo have to make?

Jo has to decide whether or not it's a smart idea to look for a boyfriend in *Fast Talk's* chat areas.

What should Jo look out for?

The most obvious problem with online interactions is that you can never tell whether the person you're talking with really is who he says he is. In real life, that seventeen-year-old boy in a chat room could be any age – and any gender. Kids need to recognize that the same chat areas that attract teens also attract people looking to exploit teens. This is especially the case in chat areas that focus on romance or sex.

Does Jo make the right decision? Why or why not?

Jo's decision to look for love online isn't a wise one. Although her brother managed to find a girlfriend, the smart move is to stick with people you know in the real world.

Some Chat Facts:

- A survey conducted on *Seventeen Magazine's* Web site in 2000 by two Florida professors found that 24 per cent of 12-18 year-old girls who spent at least 12 hours a week online said they had met an online acquaintance in person.

- Girls aged 11-14 interviewed by the Media Awareness Network acknowledged that although they initially protect their personal information in chat rooms, they find it impossible to do so after they began to feel comfortable with a person. The time it took them to begin to trust an online stranger ranged from several weeks to 15 minutes.

- According to *Online Victimization: A Report on the Nation's Youth*, a study conducted by the Center for Missing and Exploited Kids, one in five regular users of the Internet said they had received an unwanted sexual solicitation or approach in the last year.

- According to the RCMP, these are some of the strategies of online predators:

  - Creating an atmosphere of trust with a potential victim by listening to a kid's problems and empathizing with them

  - Attempting to overcome young people's inhibitions by gradually introducing sexual content into their conversations, or by e-mailing them sexually explicit material

  - Eventually, attempting to make contact with the child in the real world

Additional Questions and Discussion

Before discussing the negative aspects of chat rooms, ask students to brainstorm the positive aspects of chat. For example, chat:

- builds online communities

- is a great way to connect with people from all around the world

- lets you be judged by what you say, not how you look

- is lots of fun

Ask students to list their favourite chat environments. Then read the "Chat Facts" to the class, and ask them:

- How do you feel about these statements? Do you think they're accurate?

- How many of you have participated in online chat?

- How many of you have visited monitored chat rooms, where a moderator oversees the conversations to make sure that language and behaviour are appropriate?

- How many of you have visited unmonitored chat rooms, which have no such restrictions? For those who have participated in both types, which do you prefer? Why? Are the favourite sites monitored, unmonitored, or both?

- Have any of you ever been harassed, or sent disturbing messages, in chat environments?

- If you were harassed, what did you do about it? What could you do about it? Options include reporting it to the Web site, telling an adult, reporting it to your ISP provider.

- Remember those girls who said they had difficulty protecting their identities after chatting to someone for while? Do you think it's safe to give to someone personal information about yourself you've met online?

  - What kind of information?
  - When is it safe to do this?
  - How can you tell if a person is trustworthy?

- How many of you have met an online acquaintance in person? How did it turn out? What precautions did you take to protect yourself? Did you check it out with an adult first, and have the adult come along? Was the meeting in a public place?) Brainstorm some safety rules for real-life meetings with online acquaintances.

- Using the Media Awareness Network's search engine, check out the RCMP's description of Online Predators. The familiar online acronym for finding out a person's age, sex and location (A/S/L) can be very useful in helping predators select a potential victim. Many predators look for kids of specific ages and genders. (This is why it's important that your online identity be age- and gender-neutral – and certainly not sexually suggestive, that's just asking for trouble!) Ask students to share their e-mail or online identities, and decide how good a choice they are from an online safety perspective.

- Predators often get information about kids by asking leading questions – questions that sound innocent, but are intended to help them decide if someone's a promising target. Watch out for questions that ask for specific information about your address, school, what teams or clubs you belong to, or your family. Remember that predators are pros – they will often find very subtle ways of getting the information they want. A predator may say something like: "The only time I get to chat online is after school, before my mother comes home from work. Do your parents hassle you about going online after school?" This question sounds pretty innocent, but it's actually fishing for information on whether you're home alone. Ask students to brainstorm examples of other leading questions.

- Predators are very good listeners, and they love kids with problems – because chances are, those kids are looking for someone to talk to. Predators will empathize with your feelings: if you're sad, they understand; if your parents are ogres, theirs are too. Watch out for "instant soul-mates" who seem too good to be true. Also watch out for excessive flattery.

- In order to cultivate your trust, predators are eager for "one on one" conversations. The easiest way to avoid this is to keep all online conversations in the main areas, which are open to all participants. Don't ever offer your personal e-mail address to an online acquaintance – instead, offer to meet him/her again in the same public chat area.

Activity

Divide the class into groups.

In this session, we've talked a bit about the positive side of chat, and we've looked at some of the problems faced by kids and teens in chat environments. For this assignment, you will take on the role of a task force responsible for finding a solution to these problems. As a group, you will develop a presentation to an international committee studying online chat. The presentation will:

- Outline the positive aspects of chat

- Outline the problems associated with young people and chat

- Offer some creative solutions to these problems, identifying the roles to be played by parents, kids and teens, governments, Internet Service Providers, and Web sites

- Provide a set of safety guidelines for kids and teens who participate in chat environments

Ask groups to make their presentations to the class and discuss their findings.

Online Safety Scenarios

Jo's Home Page

The Web provides many opportunities for users to create their own personal home pages. Many Internet Service Providers offer free Web pages as part of their subscription services. Teens in particular enjoy creating their own Web sites to share interests and meet new people. A home page can be a wonderful form of self-expression, but these pages can become problematic when young people inadvertently reveal too much personal information.
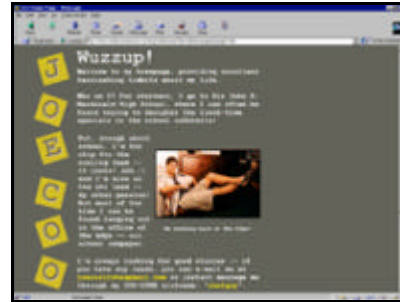
What kind of Web site is this?

Personal pages on any topic under the sun can be created easily and inexpensively by anyone who has access to the Internet. Many kids and adults use personal pages featuring hobbies and interests as a means of networking with people who share the same interests.

What decision does Jo have to make?

Jo needs to figure out how to create a home page that doesn't put his personal safety at risk and that respects the copyright status of material he's borrowed from other Web pages.

What should Jo look out for?

Some kids create pages to share with their friends, forgetting that anyone in the world can access their material once it's posted to the Web. Problems can occur when young people offer too much personal information online. Jo should be aware of this on his own page.

Does he make the right decision?

On this page, Jo describes his hobbies, offers contact information, identifies the city and street where he lives, the school he attends, and provides family information and a photo of himself. This information makes it very easy for someone to contact him – online or in the real world.

Luckily, Jo is more conscientious when it comes to respecting copyright. For his "Sens Shrine" page, Jo asked permission from the Ottawa Senators before downloading and posting images from their Web site. He has acknowledged that these images are registered trademarks for the team, he has acknowledged the source of these images and confirmed that they are posted with permission, and he has provided a link from his page to the Ottawa Senators Web site. Just because this is a personal page, that doesn't mean Jo can use other people's materials without permission. If he posts something online that belongs to someone else, he must ask permission first and credit the source.

Another issue that relates to personal pages is quality of information. People can create Web pages that look very impressive and credible, even if they're not! When you're conducting research online, it's important to confirm the accuracy and credibility of any information you encounter.

Additional Questions to Ask Students

During this discussion, write students' answers on the board in order to create an overview of the number of personal Web pages; the most common themes; the kinds of personal information posted; how many students use images downloaded from other Web sites; and how many respect copyright.

- How many of you have personal Web pages? (If a computer lab is available, students may want to look at the pages their classmates have created.)

- What's the purpose of your site?

- What kind of information do you post on your page?

- Is any of it personal?

- If you do post personal information, do you feel that putting this online compromises your personal privacy? Why or why not?

- If you have posted contact information on your Web page, has someone ever contacted you? What was your experience?

- Are any images used on your page?

- Did you get these images from another Web page?

- If so, did you ask permission? How?

- Does your site acknowledge this permission, credit the source, and provide a link to the original owner?

Student Web Sites and Free Speech

A growing area of concern is student Web pages that contain rude or threatening comments and jokes about classmates and teachers.

- Do you feel that schools should hold kids accountable for school-related comments made on Web pages created at home?

- How would you categorize the following scenarios: acceptable, in bad taste, cruel or illegal?

  - a page that posts nasty rumours about students and teachers

  - a page naming the sexiest girls or guys at school

  - a page naming the ugliest girls or guys at school

  - a page that contains mock obituaries of students

  - a page containing cartoons showing a student or teacher being killed

 - a page with racist or sexist comments about teachers or students

What would the appropriate consequences be in each of these cases? If your school has policies on appropriate online conduct and consequences, you may want to review and discuss these with students.

- Write a paragraph responding to the question: "When does free speech cross the line?"

Because online safety is a serious issue, some awareness campaigns can be pretty heavy-handed. Ask students to come up with an Internet Safety Awareness Campaign that uses humour to help other kids understand any one of these safety issues:

- the importance of safeguarding personal information in chat environments and on Web pages

- how to recognize when you're being targeted online, and how to avoid it

- what to do if you encounter an online situation that makes you feel uncomfortable or scared

- how to recognize safe Web environments

- how to conduct effective Web searches that minimize exposure to inappropriate materials

Students can create posters or collages for school computer rooms and libraries. For example, the Ottawa software company Kyberpass created this poster as a humourous way to remind people that you never know who you're chatting with online:
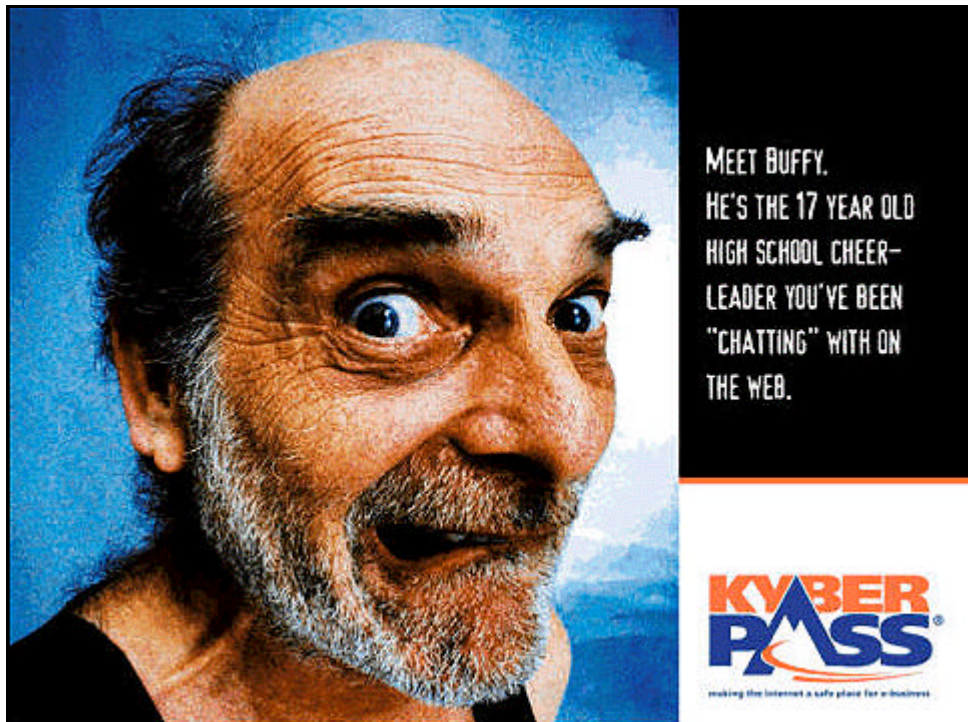
Authenticating Online Information

The popularity of the Internet as a homework resource has created a whole new challenge for young people: how can they know what online information to trust? Librarians note that young people who are perfectly adept at using technology to *find* information are often lost when it comes to *evaluating* it.

❖ **Who** is the source?
❖ **What** are you getting?
❖ **When** was it created?
❖ **Where** are you?
❖ **Why** are you there?
❖ **How** can you tell what's what?

As one American librarian puts it: "Show students a list of the presidents out of order on a Web site, then show them the correct listing in a book. They'll believe the computer."

> **According to the Media Awareness Network survey *Young Canadians in a Wired World*, less than three in ten secondary school students double-check the information they find online. Of the students who do take the time to verify online information, half say they "judge for themselves" whether it's accurate.**

As we move into an age in which more and more information is accessed through the Internet, it's crucial that young people develop the critical thinking skills they need to evaluate the quality – and just plain truth – of what they find online. Unlike the traditional publishing process, creating a Web site is relatively simple and inexpensive. There are often no gatekeepers for this medium – no editors or publishers – and everyone can post their views. So it's important to know how to check the credibility of a source before accepting information as fact.

Students also need to learn to recognize bias – to understand the relationship between the purpose of a site and the slant of its content. Is the purpose of a Web site to inform? To sell? To entertain? To persuade? What information is missing? Are other viewpoints offered? Web sites should clearly state their purpose and goals – but this is rare. Even when they do, it's important that students question the information in terms of bias and accuracy.

> **When it comes to finding information for homework, 44 per cent of young people turn to the Internet first, over books from schools and libraries.**
>
> **Source: Young Canadians in a Wired World**

Young people need to appreciate that the Internet is only one resource of the many available to them. They also need to understand this medium's strengths and weaknesses. For instance, some Web sites that look quite substantial provide only superficial information. And although the Web is an excellent source of fast-breaking information, currency does not guarantee accuracy. Thorough research includes both text-based and computer resources.

Traditionally, kids have been taught how to find resources in their school libraries. Now they need to develop effective online search strategies as well.

The Media Awareness Network's 5 Ws of Cyberspace (which can be found in the Fact or Folly section of Web Awareness for Teachers) encourages kids to measure the quality of Web resources by asking:

- Who is the source?
- What am I getting?
- When was the site created?
- Where am I?
- Why am I here?
- How can I tell this is a quality Web site?

We can all be fooled in our online explorations. But, if children are taught to approach Internet information with a healthy scepticism, they can develop a critical eye and mind.
_____

Jo Cool Scenarios for Authentication of Information

The following scenarios address authentication of online information: Homework Nook (page 23), Teen World (page 25), Cheapmail (page 27), Summer Daze (page 29).

Additional Resources

Background materials for teacher:

- MNet's Fact or Folly section (in Web Awareness for Teachers) contains information and resources on this topic.
- For teachers who want to know more about authenticating online information, the Web Awareness for Teachers section also includes the professional development workshop Fact or Folly: Authentication of Online Information.
- Evaluating Internet-Based Information (which can be found in the Fact or Folly section of Web Awareness for Teachers) is a goals-oriented approach to Internet research projects. It includes an "Internet Information Evaluation and Collection Form" that can be downloaded and used in the classroom.

Lessons and Handouts – access the following lessons using the Media Awareness Network's search engine:

- 5 Ws of Cyberspace helps students authenticate online information by using the tried and true "5 Ws" of journalism: who, what, when, where, why – and how.
- Deconstructing Web Sites shows how to deconstruct a Web page in order to determine its credibility as a source of information.
- Quick Tips for Authenticating Online Information offers step-by-step instructions to authenticate information using Meta Web Information searches.
- ICYouSee: T is For Thinking is a lesson that helps students critically analyze information they find on the Web.
- A Tale of Two Cities is a "teachable moment" that demonstrates the importance of authenticating online information.
- Teaching Zack to Think is a case study of a student who encountered a hate site on the Internet.

Authenticating Online Information Scenarios

Homework Nook

Jo comes across *Homework Nook* while conducting an online search for "human rights." *Homework Nook* is actually a white supremacist page that blames the Canadian Human Rights Act for taking jobs from white people. Like many similar sites, *Homework Nook* doesn't state its purpose outright, but rather presents itself as being an unbiased examination of a particular issue.

What kind of Web site is this?

Jo thinks he's visiting a general homework site. In fact, it's the personal home page of "Professor Earnest Dumbell."

What decision does Jo have to make?

Jo has to decide whether the material on this site is a valid resource for his homework assignment.

What should Jo look out for?

There are a number of references in the text of this page that indicate bias and subjectivity. Jo should recognize the bias in statements like "difficulties faced by white people," "today's biased society" and "subversive laws." He should check to see if the site provides links to alternative view points. He should question the credibility of the author: who is Earnest Dumbell? Is he even a professor? What makes him an authority in this area? Jo should note that the opinions expressed by the author are not widely held opinions in Canadian society. This doesn't necessarily mean they are wrong, but it does mean they shouldn't be accepted as fact without asking a few questions first.

Strategies Jo could use to verify the credibility of this site's creator include conducting a Web search on the author's name. Chances are, if Earnest Dumbell is a known hate-monger, this will become apparent in the search results. Students might also "link" in the search command box, followed by the full address of the site in question. This search will tell you what other sites link to this one. If *Homework Central* is really a hate site, results might include online articles about hate on the Internet and Web sites for watchdog organizations that monitor hate on the Net.

Does Jo make the right decision? Why or why not?

In this case, Jo doesn't recognize hate for what it is. We expect online hate to be quite obvious, but it can often take subtle forms on the Internet.

Examples we've found include:

- **a respectable-looking Web site dedicated to Martin Luther King, <www.martinlutherking.org>, produced by the White Supremacist group Stormfront**

- **a Pokemon page on Stormfront's kids' page <http://kids.stormfront.org/pokemon/index.html>**

- **a kids' page that promotes white power through games and crossword puzzles <http://216.221.171.242/kids/main.html>**

Because many kids lack the life experience to refute the information on these sites, it's important that they make a habit of questioning all online information before accepting it as truth.

Additional Questions to Ask Students

- Can you think of different types of hate groups that might promote their beliefs on the Internet? These might include groups that promote hatred against different races, against women or men, or against different religions and cultures.

- Can you think of other examples of online hate? Some Web sites might promote hatred against individuals: a student page that slams teachers or students, or a page that makes threats or incites hatred against a celebrity.)

- Have any of you ever encountered a Web site promoting hatred? How did you feel when you encountered it? Did you do anything about it?

- What about a Web site that features lyrics by a controversial artist or rapper like Eminem? Because this person is a popular performer who's allowed to perform these songs in public, do these lyrics constitute hate when they're posted on the Web?

- Are hate sites illegal, or just hurtful? According to Jeffrey Schelling's book *Cyber Law Canada*, the Criminal Code of Canada now includes three offenses Web sites can commit that qualify as hate crimes:

  - advocating or promoting genocide
  - inciting hatred against identifiable groups,
 - willfully promoting hatred against an identifiable group

These are all considered illegal in Canada. (Web sites that advocate violence against individuals, or that threaten them, already fall under Criminal Code statutes dealing with assault, harassment and threats.)

Authenticating Online Information Scenarios

Teen World

Teen World is an online e-zine that offers contests and information that appeal to teenagers. Celebrity gossip, hair and fashion talk, online surveys, bodybuilding tips, live chat and articles on topics such as computer hacking are all intended to lure visitors and encourage them to register and interact with the site.
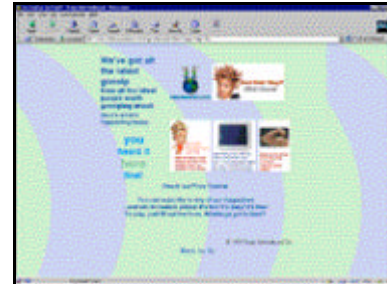
What kind of Web site is this?

In this scenario, the e-zine *Teen World* is a non-branded commercial Web site, supported by advertisers who pay for ads on its pages. Although *Teen World* has its own domain name, a quick look at the copyright information tells you that it is actually owned by a company called *Rags International*.

What decision does Jo have to make?

Jo has to determine the reliability of information found on this Web site.

What should Jo look out for?

Teen World is nothing more than a sophisticated marketing vehicle for advertisers. Jo should watch out for bias, and for relationships between the content on the site and the advertisers that support it. For instance, does the "hair care" section only promote "Permanent Rave" products? Are the bodybuilding tips connected to the "Mega Muscle X-treme" line of supplements? What about those harmless-looking surveys? Does *Rags International* share these surveys with third parties such as marketers?

Jo also has to consider the credibility of the author or source of this Web site: *Rags International*. She knows that this company has been in trouble for altering photos and posting them online. The fact that this Web site features an article that promotes hacking is also a good indication that Jo should question the integrity of *Teen World*.

Does Jo make the right decision? Why or why not?

Jo makes the right decision in giving *Teen World* a pass. She recognizes that the information on this Web site most likely contains bias – and, judging by the track record of *Rags International*, she knows that the quality and accuracy of its articles are questionable.

Additional Questions to Ask Students

- How can you find out who's behind a Web site? The first step would be to check out any "about us" information. Other options include checking out the privacy policy or even the e-mail address in the "contact us" links. As a general rule of thumb, if you can't establish the credibility of the organization or author behind a Web site, don't use it.

- What is bias?

- How can you recognize bias on a Web site? A few signs might be:

  - a relationship between the perspective of the authors and the organization they represent

  - using emotion, rather than logic to persuade readers

  - the use of broad terms and unsubstantiated language

  - only one viewpoint is expressed

  - no links are provided to other viewpoints

- Have you ever participated in an online survey? Where did you find it?

- What was the survey about?

- Did the Web site tell you what would be done with any information collected?

- *Teen World* offers tips on hacking. Is this illegal in Canada? (The Criminal Code considers the following to be illegal: unauthorized alteration, destruction, or interference with the use of data; unauthorized access to, or use of, a computer system; and unauthorized interception of computer communications. Teen World could be found liable for counselling people to commit a crime by offering tips on hacking.)

- What are some examples of hacking? Students should understand that using their friends' instant messaging or e-mail passwords without permission to access their accounts or to assume their identities online is a form of hacking.

**Authenticating Online
Information Scenarios**

Cheapmail

Web-based e-mail services like *Cheapmail* are immensely popular with young people. These remote services permit users to access their e-mail accounts from any computer. In order to obtain an account, users register with the Web site.
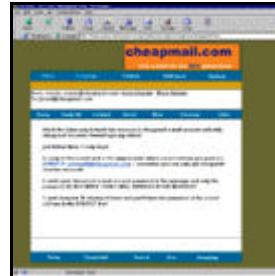
What kind of Web site is this?

Web-based e-mail services like *Cheapmail* offer free remote e-mail accounts to users. These sites are usually supported by advertising dollars, and many offer a wide range of services that include instant messaging, shopping, online directories, search engines and chat.

What decision does Jo have to make?

Jo has received a message offering to provide her with the password to someone else's *Cheapmail* account. All Jo has to do is submit the e-mail address of the person whose password she wants to a person called hackz_crackz, and she will receive the password within the next four hours. Jo has to decide whether she wants to do this.

What should Jo look out for?

E-mail accounts like *Cheapmail* are very convenient, but there is a downside to services like these. If not careful, users may compromise their personal information – or they may find themselves bombarded with unwanted spam from explicit adult sites, gambling sites and online con artists.

Careful reading exposes this scam quickly. Your first hint that something may not be right is the offer itself – hackz_crackz is offering to help you do something that is not only wrong, but illegal under Canadian law. On that premise alone, this message should be ignored.

There are also holes in the logic of this message. Why would hackz_crackz need your e-mail password to begin with? The warning that you need not include your own e-mail address in your return message sounds reassuring, until you realize that this information is automatically included at the top of your reply message.

To avoid unwanted spam, never respond to unsolicited e-mail. By even sending a message back, you're verifying your e-mail address is valid. Forward any offensive e-mail, junk e-mail or "spam" to your Internet Service Provider (ISP); and report any e-mail that contains illegal material (such as threats or child pornography) to your local police.

It's also a good idea to use e-mail filters. Many e-mail programs have features that allow you to filter out messages from particular people, or containing specific words or phrases.

Does Jo make the right decision? Why or why not?

Josie is wise to pass on this one. She would be even smarter to forward this e-mail to her *Cheapmail* service provider.

Additional Questions to Ask Students

- How many of you have Web-based e-mail accounts?

- Have any of you received spam in your accounts?

- What kinds of spam do you receive?

- How do you handle the spam?

- Have any of you used filtering or blocking options to prevent spam? Has it made a difference?

- Why are online passwords so important?

- Do any of you share your e-mail passwords with friends?

- What are some potential problems with doing this?

- Is what hackz_crackz is proposing improper or illegal? (According to the Criminal Code of Canada, it's illegal to interfere with computer communications like e-mail, and to access someone's online account without consent.)

Extension Activity

If computers are available, students might visit Web sites like Hotmail or Yahoo and take a look at the available filtering and blocking options. Students should also look at the registration process to see if any default settings need to be activated to protect their privacy. In March 2001, Hotmail came under fire because of its practice of setting its default settings to automatically include users' Hotmail addresses in its online Directory and Internet White Pages – which were then sold to marketers.

Authenticating Online Information Scenarios

Summer Daze

When Josie visits *Summer Daze Tour*, a Web site promoting a fantastic rock concert, she's all set to buy tickets, hop into a van with friends and head out to California. It sounds like it's going to be an exciting event: 40 big-name bands and rock artists, and lots of hype! The question is, will *Summer Daze* live up to its billing?

What kind of Web site is this?

This is a promotional Web site. Many organizations use the Internet as a cost-effective way to promote everything from concerts to conferences. Promotional Web sites like *Summer Daze* are quite common online.

What decision does Jo have to make?

Jo has to decide whether or not to purchase a ticket to attend this concert.

What should Jo look out for?

As Jo discovers, it's very important to check out both the event, and the organization behind it, before submitting any money. This site looks quite legitimate. It sounds like a large-scale, well-planned event ("Six years in the making!"), features newspaper headlines from reputable papers, and provides a mailing address and a phone number. However, it's still important that Jo do her homework before sending in money for tickets. Ways to do this include contacting the Better Business Bureau; going to the official Web sites for some of the artists billed, to see if their concert listings include this venue; checking out the official Web site for Carmel California to see if the concert is featured as an upcoming event; checking out the newspapers mentioned for information about *Summer Daze*.

Does Jo make the right decision? Why or why not?

Jo falls for the illusion of legitimacy. Because this sounds like such a large event, and all her friends are planning on going, Jo lets her enthusiasm get the better of her. She forgets that on the Internet, scepticism should be your rule of thumb.

Activity

- Have students visit the Web site of the American Federal Trade Commission, and check its "Top Ten Dot Cons" page at www.ftc.gov/bcp/conline/edcams/dotcon/index.html. As an assignment, students can summarize in their journals how each of these online scams operate – and mention what individuals can do to minimize the risks. Or, they can form groups to research one of these scams in more depth and present their findings to the class.

Responsible Internet Use

Conveying the concept of online responsibility is one of the biggest challenges for educators.

On the negative side, anonymity can embolden adolescents and teens, who see cyberspace as a place where they can vent, act out, and participate in risk-taking activities with no consequences.

> **A recent survey in the U.S. found that 48 per cent of students in elementary and middle schools don't consider hacking illegal.**
>
> **Source: abcnews.com**
>
> **According to *Young Canadians in a Wired World,* nearly half of Canadian adolescents between the ages of 9 and 17 have visited a Web site with violent or gory pictures.**
>
> **Nearly two in ten Canadian young people admitted posting comments on the Internet that were hateful toward a person or group of people.**
>
> **In winter 2000, a Vancouver elementary school principal suspended eight students in Grades 6 and 7 for posting a Web page containing racist, homophobic, sexist and derogatory statements about children in the school.**
>
> **Source: Ottawa Citizen**

Irresponsible online behaviour ranges from actions that are inappropriate, dishonest or unkind, to those that are dangerous or illegal. Examples include:

- obtaining a commercial software program from the Net without paying for it

- plagiarizing materials

- downloading and using images or graphics from Web sites without permission

- creating Web pages or sending messages that insult or threaten others

- creating Web pages that promote hacking, bomb-making, drug use, or other illegal activities

- stealing passwords and hacking into Web sites, e-mail or Instant Messaging accounts belonging to others

- assuming someone else's online identity

- deliberately participating in chat rooms or visiting Web sites, that deal with explicit adult themes

It's important that young people understand the concept of online ethics and the importance of being good "Netizens." Today's students *are* the Internet generation, and *should* play an active role in determining the kind of virtual world they want to participate in.

A good beginning is to encourage young people to discuss "real world" citizenship, and then apply it to the virtual world.

What are the codes of conduct asked of ourselves and others in our schools and communities? We are expected to:

- treat all people with courtesy and respect

- be active participants in society

- respect the privacy of others

- respect the property of others

- obey the law

These codes can all be applied to Internet conduct, or *"*Netiquette*"*, as well.

- treat all people with courtesy and respect in chat, e-mail or Instant Messaging

- don't "flame" or personally insult individuals or groups

- don't post rude or insulting materials on personal Web pages

- respect the privacy of others: don't read the in e-mail without permission

- don't use someone else's password without permission

- safeguard and protect your own privacy

- treat school computers with respect

- do not disable filtering software that has been installed on school or home computers

- don't hack into anyone else's Web sites, directories, e-mail accounts, or instant messaging accounts

- don't use anyone else's materials, images or graphics without asking permission and crediting the source

- remember that ignorance is no excuse for not obeying the law. Know the laws pertaining to:
  - Web sites that promote hate, obscenity, hacking, weapons or drugs
  - online stalking
  - online threats
  - defamatory statements
  - harassment
  - copyright infringement

- get to know the laws that protect our privacy on the Internet

- get to know the laws that protect the safety and rights of young people when they go online

- be active participants in society

- become aware of Internet issues and debates

- know where to go and what to do if you wish to voice concerns

- find examples of youth activism on the Internet

It's important for young people to understand the possible consequences of breaking the law in cyberspace. Many believe there are no consequences for illegal or inappropriate online activities. They consider computer mischief harmless, and use the excuse "I was only joking" to justify insulting or threatening peers in chat, instant messaging or e-mail. Parents, teachers and community police should work with young people to promote accountability online.

The following activities help to reinforce in kids' minds the need for responsible online behaviour, and their roles as active Net citizens:

- invite a community police officer or a lawyer to talk to students about Canadian laws on online activities such as hacking, advocating hatred or violence against groups or individuals, online threats and harassment, and copyright infringement

- discuss your school or school board's code of conduct for students, and how it relates to computer use

- create online scenarios dealing with ethical issues and have students debate them (Mafia-boy or the case against Napster would be excellent topics for students to discuss)

- reinforce the idea that real-world codes of conduct also apply online. What elements of citizenship in the real world would students like to see applied in the virtual world?

- find and discuss real-world scenarios that students can apply to online activities. For instance, how is walking into a neighbour's house without permission, rifling through their belongings and snooping through their personal files different from breaking into someone's Web page and looking through their private directories?

- Have students research national and international organizations that oversee user conduct on the Web. (This could include organizations such as the Canadian Association of Internet Providers <www.caip.ca/>, Internet Content Rating Association <www.rsac.org/> and the Government of Canada's Canadian Strategy to Promote Safe, Wise and Responsible Internet Use <www.connect.gc.ca/cyberwise>.)

- Talk to students about the difference between "illegal" and "offensive online material," and cite examples. (For instance, how would students categorize a Web site posting misogynous, violent lyrics from a rap CD that's sold in a record store?)

- Ask students to respond to the question: "Just because something is legal, does that make it right?"

_____

Jo Cool scenarios for responsible Internet use

In addition to the following resources – ICU-UCME (page 30), Votingbooth.com (page 34) and Essay World (page 38) – educators can also use Cheap Mail (page 27) and Jo's Home Page (page 18) to explore responsible Internet use.

Additional Resources

Background materials for teachers:

- The Safe Passage section in Web Awareness for Teachers contains many resources on this topic, including:
  - General Internet Guidelines for students
  - Information on Acceptable Use Policies

- How to track where kids have been on the Internet

- Internet Censorship: Issues for Teacher-Librarians

- How to Discourage Plagiarism, a Fact or Folly tipsheet, features guidelines for teachers to help minimize online plagiarism.

  For teachers who want to delve into responsible Internet use in more depth, the Web Awareness section for teachers features the professional development workshop: Safe Passage: Teaching Kids to be Safe and Responsible Online

Lessons and Handouts – access the following resources using the Media Awareness Network's search engine:

Handouts:

- Internet Checklist for Kids, ages 9-12
- Internet Checklist for teens, ages 13-17

Lessons:

- For students in Grades 6-7, MNet offers the computer game Cybersense and Nonsense: The Second Adventure of the Three CyberPigs, the sequel to *Privacy Playground*. This game helps children recognize stereotyping, prejudice and bias on the Internet as they evaluate the authenticity and truthfulness of online information. The game, and an accompanying Teacher's Guide can be downloaded from the site onto a classroom computer.

_____

Other Web sites that address responsible Internet use include:

- Cyber Citizenship
  www.cybercitizenship.org
- Plagiarism Theme Page
  www.cln.org/themes/plagiarism.html
- Copyright Matters
  www.cmec.ca/else/copyright/matters/indexe.stm
- Teaching Students Right from Wrong in the Digital Age
  www.doug-johnson.com
- What Every Teacher Should Know About Copyright
  www.2learn.ca/copyright/copy.html
- Responsible Netizen
  http://netizen.uoregon.edu/

ICU-UCME

ICU-UCME is an Instant Messaging service that lets kids have real-time conversations with friends online. Software like ICU is very popular because, unlike chat rooms, it permits users to customize "buddy lists" of friends. Instant messaging software lets users know when a friend is online so they can chat. Many people feel that instant messaging is a safe alternative to chat environments, and it can be. But this software has shortcomings that young users should be aware of.
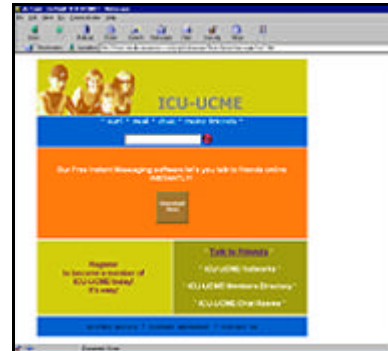
What kind of Web site is this?

ICU-UCME **is a commercial Web site that offers instant messaging services to registered users. Web sites like** *ICU-UCME* **usually provide other services as well, such as open chat environments, directories, online stores and e-mail services.**

What decision does Jo have to make?

Jo's brother, Jay, gets into an argument online with his friend Matt. Matt thinks Jay has insulted him. Jay thinks his friend is over-reacting. Jo asks students to decide who's right.

What should Jo look out for?

Online conversations are different from real-world discussions. Many kids who use language unique to this online environment, such as LOL ('laughing out loud") or little emoticons such as "smilies": :-). But even with these indicators, online conversations can be problematic. Because participants can't read the facial expression or tone of voice of the person they're chatting with, conversations can easily be misinterpreted. This is especially true of sarcastic humour.

Kids also need to understand that we respond to the written word differently from the spoken word. A verbal gaffe in a live conversation might be overlooked, but the same gaffe in a written conversation lingers on the screen and is harder to ignore.

Understanding "Netiquette" – proper online conduct or manners – is important. In this scenario, Jay makes a general disagreement about snowboarding into a personal one by engaging in name-calling. Good Netiquette stresses the importance of avoiding personal insults (or "flaming") in online conversations.

Does Jo make the right decision? Why or why not?

This scenario ends with some tips for conduct in instant messaging and chat

environments:

- **treat other people with respect**

- **don't make personal comments about others – keep conversations general**

- **don't make personal "jokes" about others online – they often fall flat**

- **don't put up with insulting behaviour. Use your "block" mechanism to prevent people you don't want to chat with from contacting you**

Additional Questions to Ask Students

- How many of you participate in Instant Messaging?

- What are the advantages of Instant Messaging? How is it different from, or similar to, online chat?

- What are the disadvantages of Instant Messaging?

- Although instant messaging can be fairly safe, there are issues that teens should be aware of. Shortcomings of instant messaging include exposure to objectionable materials; receiving virus-contaminated files that may infect your computer; and unauthorized use of your IM name or password. Also, many popular instant messaging companies offer chat environments that may not be suitable for kids and teens; and some include "roaming" options that permit kids to search for and receive messages from anyone in the world. There are privacy issues as well. In the process of setting up instant messaging, participants must complete registration forms that can be quite invasive.

- How many people do you have on your buddy lists? How many online buddies are friends you know in real life? How many are online acquaintances? How did you acquire these online acquaintances?

- Have you ever had to block someone from your list – or been blocked yourself? What happened?

- This scenario features Netiquette rules for chat and Instant Messaging. Can you think of other rules for good Net manners?

Extension Activities

- To register for instant messaging (and other online activities), users are often asked to complete online registration forms that ask for unnecessarily detailed information. It's important that young people learn to "read the fine print" in order to avoid disclosing too much information, and in order to understand the terms and conditions associated with using the software. Review and discuss the Kids for Sale tip sheet Filling Out Online Registration Forms with students.

- Ask students to share examples of acronyms or emoticons they use when they're Instant Messaging or chatting online. Then write or draw some on the board and see if students can guess what they mean. (You could divide the class into two groups, and give each team a list of "cyberspeak" terms and definitions to stump the other team with; or you could write a paragraph on the board and have your students rewrite it in "cyberspeak.") Examples of some terms and "smilies" can be found on the Computer User High Tech Dictionary and Net Lingo Web sites. (As some of these terms can be rather rude, teachers may want to pre-select those they want to use in class.)

  - High Tech Dictionary emoticons
    www.computeruser.com/resources/dictionary/emoticons.html
  - High Tech Dictionary chat acronyms
    www.computeruser.com/resources/dictionary/chat.html
  - Net Lingo emoticons
    www.netlingo.com/smiley.cfm
  - Net Lingo acronyms and shorthand
    www.netlingo.com/emailsh.cfm

Responsible Internet Use
Scenarios

Voting Booth

Voting Booth is a Web site that allows users to create an instant voting booth where visitors can vote on a variety of subjects. Students from across North America use sites like this to create booths for their schools on topics such as the "coolest boy or girl" in a class, "favourite celebrities" or "coolest bands."

What kind of Web site is this?

Voting Booth provides a free service to visitors that allows them to create virtual "voting booths" where Web surfers can come and vote on a wide variety of topics. Web sites like these are supported through advertising dollars.

What decision does Jo have to make?

Jo has created a booth on "the most popular teacher at Sir John A. MacDonald High School", and has listed several teachers whom students can vote for. Students must decide whether Jo has acted wisely.

What should Jo look out for?

Many of these booths are harmless, but problems can occur when booths are created that degrade individuals; or when visitors add offensive or hateful comments or categories to existing booths.

Jo can control the topic she selects, but she may not be able to control the comments submitted by others to her booth. When you create an online voting booth, an option button is usually provided to let visitors add their own categories or comments. If you want to be sure that people don't add offensive or inappropriate comments to your booth, click "NO" for this option.

Online voting can be fun if you avoid topics that identify real people or are rude or insulting. Choosing topics like "Most Popular" or "Hottest Guy/Girl" at your school are asking for trouble. Stick to neutral territory.

Staff for sites like Voting Booth will monitor booths for inappropriate content, and users are expected to abide by the site rules. Still, there have been instances in Canada where students have been suspended for creating booths that slandered other students or teachers.

Does Jo make the right decision? Why or why not?

Jo learns the hard way that things can get out of control very quickly if you're not careful. It pays to read the rules and think carefully when participating in online activities like these.

Extension Activity

For each of the following scenarios, have students role-play the perspectives of the offending students, the students or teachers who are victimized, students' parents, school officials, and law enforcement officers.

Ask students to explain what the appropriate consequences should be in each case. (Teachers might want to use their school or school board's Acceptable Use Policy as a reference.)

Scenario One

Several students have created a gossip site about their high school (GHS). They created the site from a home computer, and will print anything other students e-mail to them. The items posted are often immature, cruel and mostly untrue – and they identify specific kids by name. Most of the students at GHS have visited this site.

To protect themselves, creators have posted the following disclaimer on their site:

> *GHS News Disclaimer*
>
> *If you think you will find any material on this Web site offensive in any way, DO NOT ENTER. The names, incidents, and views expressed within are not necessarily true, but in some cases may be. This is not an authorized Web site for our High School. We are not to be held responsible for any of your actions. Please do not go to our Web site while in school. If you choose to go to this Web site during school hours, it is at your own free will. We highly discourage the viewing of this site (or its printed material) during class time, school hours, or anywhere on the school premises. We also discourage anyone from talking about this Web site (or its printed material) during class time, school hours, or anywhere on the school premises. Doing so is also at your own free will. Thank you.*
>
> *-GHS NEWS*

A student discovers that someone has posted an untrue message about her saying that she does drugs and sleeps around. Soon everyone at the school is talking about it. Her parents find out and are furious. They go to the school principal.

Scenario Two

A student creates an "I Hate My School" site. On it, he identifies students and teachers he doesn't like, and posts rude and insulting comments about them. He also posts some cartoons he's drawn of shooting targets with pictures of the students and teachers he dislikes in the middle of them. A number of these cartoons get printed by his friends and are posted around the school. His home room teacher discovers them, and arranges a meeting with the student, his parents, and the school principal.

Scenario Three

Two students create a voting booth where kids from their school can vote on the best looking guy and girl in each class. Instead of getting what they expect, many of the students who participate add rude, insulting and even threatening comments about their classmates. Before the students have a chance to remove their booth, it gets discovered by school administration. Because they are the booth's creators, these two students are held responsible, even though they didn't post anything offensive themselves.

Responsible Internet Use
Scenarios

Essay World

Essay World is a plagiarist's dream. It's one of many Web sites that permit visitors to purchase or download essays and research papers. The quality of papers available online ranges from essays submitted by students to those created by professional writing services.

Jo discovers *Essay World* through his friend Jason. It's pretty tempting – will Jo go for an easy grade? Or will he slog it out and write the essay himself?
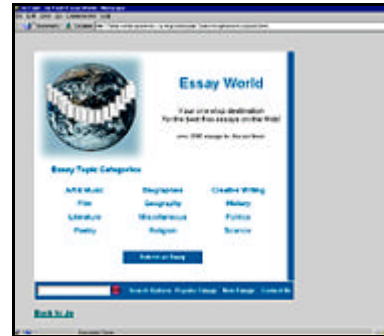
What kind of Web site is this?

Like the non-branded commercial Web sites, many free essay sites are supported through advertising dollars. Other essay sites are supported through the papers they sell.

Some of these Web sites feature disclaimers stating that their Web site is intended for research purposes, and recommend that any papers used be cited in a bibliography. Others offer essay writing services, for as much as $18 per page.

What decision does Jo have to make?

Jo has to decide whether or not to download an essay from this Web site and submit it to his teacher as his own.

What should Jo look out for?

In addition to the fact that plagiarism is wrong, there are other factors that Jo should consider:

- Many of the free essays on these Web sites are written by students. They vary greatly in quality, and some may not be very good or accurate.

- There are also questions regarding the original sources used in these essays. Are they cited correctly? Are they creditable sources to begin with? Do these essays contain plagiarised materials?

- How easy was it to find this Web site? Chances are, if you can find an essay site on a topic, so can your teacher.

- Most importantly, teachers assign research papers in order to help students develop their research and critical thinking skills. By taking a short cut like this, Jo is shortchanging himself by not developing these skills himself.

Does Jo make the right decision?" Why or why not?

Luckily, Jo makes the right decision here and decides not to cheat.

Essay World provides an opportunity for students and teachers to discuss the issue of plagiarism. Plagiarism has always existed, but the ease with which the Internet permits young people to find and download materials has added a new twist to this perennial problem.

This might be a good opportunity to review your school's policies regarding plagiarism, and to discuss the importance of citing materials properly to avoid doing this accidentally. The following Web sites offer ideas to help teachers identify plagiarism, and help students avoid it:

- Plagiarism: What It Is and How to Recognize and Avoid It
  www.indiana.edu/%7Ewts/wts/plagiarism.html
- Cut-and-Paste Plagiarism: Preventing, Detecting and Tracking Online Plagiarism
  http://alexia.lis.uiuc.edu/%7Ejanicke/plagiary.htm
- Anti-Plagiarism Strategies for Research Papers
  www.virtualsalt.com/antiplag.htm
- Copyright Matters
  www.cmec.ca/else/copyright/matters/indexe.stm
- The Fact or Folly tip sheet, How to Discourage Plagiarism.

Jo Cool Quiz

So, Jo, whaddaya know?

So you're ready to surf, eh? Been there, done that, seen it all? Well before you grab that mouse and get going, why don't you try this little quiz we've put together? Let's see if you're cool, or a…well, you get the picture! Good luck!

1. According to the Media Awareness Network, what percentage of Canadian kids and teens have met an online acquaintance in person?

   a. 6%
   b. 15%
   c. 25%
   d. 53%

2. Sixteen per cent of Canadian kids and teens have received e-mail messages that frightened or bothered them. How did most of them deal with the situation?

   a. They tried to block further e-mails from the sender.
   b. They told a friend.
   c. They replied to the sender themselves.
   d. They told an adult.

3. In chat rooms, nobody can identify you unless you want them to.

   a. True
   b. False

4. Hacking into Web sites is illegal.

   a. True
   b. False

5. You can say anything you want online – as long as it's on your own personal Web page.

   a. True
   b. False

6. If you create a Web page and want to include images from another site, which is the best way to obtain permission?

   a. You don't need to ask permission to post images from other sites on your Web page, because it's a personal page and not a commercial site.
   b. Find the contact information for the creator of the Web site and request permission by telephone.
   c. E-mail or write to the author, webmaster, or the permissions department of the company that created the Web site.

7. Which of the following would make the best password?

   a. Your pet's name
   b. A random combination of numbers, symbols and letters
   c. Your mother's maiden name
   d. Your favourite colour

8. When the American Federal Trade Commission surveyed kids' sites in 1999, what was the most common piece of personal information these sites asked for?
   a. Phone number
   b. Name
   c. E-mail address
   d. Age and birthday

9. What type of information are Canadian kids and teens <u>most</u> likely to give over the Internet to win a prize in a contest?

   a. Name
   b. Home address
   c. E-mail address
   d. Age and gender

10. Before you enter any contests on the Net, it pays to check out the contest rules and regulations.

    a. True
    b. False

11. If a Web site has a privacy policy, that means your personal information is safe there.

    a. True
    b. False

12. A "cookie" is a file that is sent to your Web browser by a Web site you've visited. "Cookies" are used on many commercial sites to track which pages users visit, and to monitor their activities. Which of these statements about cookies is true?

    a. Cookies can track which other sites you visit after you leave a particular site, and even what ads you click on.
    b. Cookies can get data and personal information from the hard drive of your computer.
    c. Computer viruses can be sent in cookies.
    d. Cookies can read your e-mail address.

13. What makes the Internet so appealing to marketers?

    a. It's popular with kids and teens
    b. The spending power of kids is worth billions of dollars
    c. It's an interactive medium
    d. It's an effective tool for collecting personal information
    e. All of the above

14. What's the best way to tell whether it's safe to submit a credit card number to purchase something from a Web site?

    a. Find and click on the small padlock icon on your Web browser.

b. See if the site you're on provides you with clear information about its security practices.
c. Look for "https:" in the Web page address.
d. Check with your parents.
e. All of the above

15. The best way to handle junk e-mail is to hit the reply button and tell them not to send you any more spam.

   a. True
   b. False

16. You've found some interesting information on a Web site. What's a quick way to check whether it's legitimate?

   a. Go to a Web server like Alta Vista and run a search on the author's name.
   b. Go to a server like Alta Vista and type in **link:** followed by the site's address.
   c. Compare what you found on the Web site to other sources on the same topic.
   d. Check it out with a teacher, librarian or parent.
   e. All of the above

17. Which of the following can't spread computer viruses:

   a. E-mails
   b. Downloadable files from Web sites
   c. Text documents
   d. Disks or CDs

18. When you're surfing the Net, Web sites can find out information about you through:

   a. Your Internet Provider (which connects you to the Internet)
   b. Your computer name
   c. Cookies that are lodged on your hard-drive
   d. The last Web site you visited
   e. The plug-ins installed on your system
   f. All of the above

19. According to MNet, what percentage of Canadian teens in Grades 7-11 believe that all information on the Internet is true?

   a. 3%
   b. 6%
   c. 36%
   d. 48%

20. Most students in Grades 7-11 take steps to confirm that the information they find online is accurate or true.

   a. True
   b. False

Jo Cool Quiz

Quiz Answers

1. According to the Media Awareness Network, what percentage of Canadian kids and teens have met an online acquaintance in person?

   a. 6%
   b. 15%
   c. 25%
   d. 53%

   a. Nice try – but if it makes you feel better, 96% of my friends got this question wrong too!
   b. You got it right! The sad truth is that 15% of the kids MNet surveyed had real-life meetings with people they met on the Net. One out of ten kids said they had a bad experience, so it makes sense to bring an adult along when you're meeting online friends.
   c. Incorrect, but close.
   d. Good news! This statistic is wrong. I'd hate to think *that* many kids don't know that arranging real-life meetings with cyber-friends is just plain dumb, unless you check it out with your folks first!

2. Sixteen per cent of Canadian kids and teens have received e-mail messages that frightened or bothered them. How did most of them deal with the situation?

   a. They tried to block further e-mails from the sender.
   b. They told a friend.
   c. They replied to the sender themselves.
   d. They told an adult.

   a. Correct. Nearly half the kids who received threatening messages tried to block further e-mails from the sender. (Most e-mail services include instructions for blocking unwanted messages.) This is a good start, but don't stop there. Harassing people online is a serious problem, so if someone is scaring you, get an adult to help you deal with the situation.
   b. You're close. Three out of ten kids who received scary or threatening e-mails told a friend about it. This isn't a bad idea, but if someone is bullying you, your best bet is to talk to an adult who you trust. He or she can report the person who's bothering you to an Internet Service Provider, or to the police.
   c. This is definitely the wrong thing to do, but 22% of kids and teens who received threatening e-mails answered the messages themselves. By answering an unwanted e-mail, you're playing into the cyber-bully's game and showing him or her that your e-mail address is correct. Don't do this. Get an adult to help you.
   d. Getting help from an adult you trust is the best thing to do if someone threatens you online – but only two out of ten kids and teens do this.

3. In chat rooms, nobody can identify you unless you want them to.

    a. True
    b. False

    a. Wrong-o! (But you're not the only one.) Lots of people think you can do or say whatever you want in chat rooms or on the Net, because no one can find out who you are. The truth is, if someone wants to know where to find you in cyberspace, there are all sorts of ways for them to do just that.
    b. You're not easy to con. The truth is that there are many ways that people can be tracked when they're on the Internet – so watch out!

4. Hacking into Web sites is illegal.

    a. True
    b. False

    a. You got it! According to Canada's Criminal Code, accessing a computer system without permission, or tampering with data, are both criminal offences. And just 'cause you're a kid that doesn't mean police don't take this seriously.
    b. Lots of kids think hacking is harmless. But in the eyes of the law, breaking into someone's Web page is just the same as breaking into someone's home.

5. You can say anything you want online – as long as it's on your own personal Web page.

    a. True
    b. False

    a. I don't think so! Because the Internet is a public place, there are many things that you can't say online – even if it's on your personal Web page. You can't threaten people online; you can't tell others that they should hurt someone or a particular person or group of people; you can't put up obscene material; and you can't tell people how to make or buy illegal weapons or drugs.
    b. **You're right. Good Netizens know that if you can't say it or do it in the real world, then you'd better not do it in cyberspace!**

6. If you create a Web page and want to include images from another site, which is the best way to obtain permission?

    a. You don't need to ask permission to post images from other sites on your Web page, because yours is a personal page and not a commercial site.
    b. Find the contact information for the creator of the Web site and request permission by telephone.
    c. E-mail or write to the author, webmaster, or the permissions department of the company that created the Web site.

    a. False. Even personal pages are considered "published" materials when they're posted on the World Wide Web. To avoid legal hassles, get permission for any pictures or cartoons you want to use. (Or better yet, make your own drawings or digital pictures; or scope out some free image sites for copyright-cleared goodies!)
    b. Asking for permission by telephone is OK if you're in a rush. Just be sure to write down the time and date of your call, the name of the person giving you permission, and exactly what you're permitted to do. Then put this into a letter and mail it to the person you spoke with and ask them to confirm the information. That way, when they respond, you will have written permission.

c. **Getting it in writing is your best way to avoid problems. In your letter or e-mail, be sure to include:**

- **a description of what you want to use**
- **where you found it on the Web site (you can cut and paste the page URL)**
- **how you plan to use this material on your Web page**
- **your name and address (if you're doing this through e-mail, this could be a return e-mail address)**

   Contact information for the author or company that created the Web site is usually found on the site's home page – but you sometimes have to do some digging! Just look for that "Contact Us" button.

7. Which of the following would make the best password?

   a. Your pet's name
   b. **A random combination of numbers, symbols and letters**
   c. Your mother's maiden name
   d. Your favourite colour

   a. Not a good idea. Avoid using information that people around you can easily identify.
   b. **Yep – this is your best bet. It's tricky to remember, but almost impossible for anyone else to figure out. I always keep a copy of my password in my sock drawer in case I need reminding – believe me, no one would dare look in there!**
   c. This isn't bad, but there's a better answer.
   d. Mellow yellow? I don't think so! That information is just too easy for someone to guess.

8. When the American Federal Trade Commission surveyed kids' sites in 1999, what was the most common piece of personal information these sites asked for?

   a. Phone numbers
   b. Names
   c. **E-mail addresses**
   d. Ages and birthdays

   a. "Reach out and touch someone?" I don't think so! 24% of the kids' Web sites the FTC visited asked kids for their phone numbers. That's pretty high – and pretty nervy – but it's not even number one.
   b. You're getting close! 74% of the sites in the FTC report asked kids for their names. They like to know who you are so they can reach out to you personally. But I prefer to keep my name for my *real* friends!
   c. **Bingo! A whopping 96% of the sites the FTC surveyed asked kids for e-mail addresses. I mean, how else can they spam you with ads, entice you back to their site or even sell your info to other companies? Before I give any personal information to a site, I check out its privacy policy with my folks – to make sure that privacy is protected!**
   d. Happy Birthday to Me? Yeah, right! 46% of the sites in this report wanted to know the ages and birth dates of the kids who visited. Excuse me for being sceptical, but what are they going to do? Throw me a party? The only gift here is the one they get from info like this: statistics on kids my age.

9. What type of information are Canadian kids and teens <u>most</u> likely to give over the Internet to win a prize in a contest?

       a. Their names
       b. Their home address
       c. Their e-mail address
       d. Their age and gender

    a. You're close. Nearly six out of ten kids and teens feel comfortable giving out their names to marketers in order to win a prize in a contest. That way they can address you by name when they send you all that spam e-mail!
    b. This is the piece of information kids are least likely to submit – only two out of ten students would give marketers their home address. A favourite trick of marketers is to ask only for your postal code. It seems like they're respecting your privacy, but this information helps them pin down the block where you live.
    c. This isn't it, although over half the kids MNet surveyed said they would give their e-mail address to a company in order to win a prize. Hello? Can you say "junk mail"? When you give out your e-mail address, you're giving marketers a sure-fire way to blitz your e-mail account with spam.
    d. **Yep, you got it. Nearly seven out of ten kids will submit their ages, and eight out of ten kids will submit their gender. It sounds harmless, but when these details are combined with other information, like your hobbies and interests, they can go a long way in helping marketers reach kids and teens on the Net.**

10. Before you enter any contests on the Net, it pays to check out the contest rules and regulations.

       a. True
       b. False

    a. **You're good at this! It really pays to read the small print. My brother found this out when he entered an online contest for some new CDs. At first, he didn't mind giving them his personal information. But he decided to take a pass on it when he clicked on the rules and scrolled all the way down to number 93, which said: "By participating, you agree to let the Sponsor use your name, address, voice, e-mail address and photograph for advertising, publicity purposes, and anything else they feel like doing – whether or not you become a winner."**
    b. Watch out! Sometimes you can get more than you bargained for when you enter contests online. I wouldn't want my name and e-mail address posted on a site for everyone to see. Read the fine print before you enter an online contest.

11. If a Web site has a privacy policy, that means your personal information is safe there.

       a. True
       b. False

    a. Guess again! Privacy policies are posted to tell you what will be done with any information you give to a site – but you have to read them to find out whether or not your personal info is protected.
    b. **Good choice! The only way you can decide if a Web site protects your info reading its Privacy Policy. Some sites are better than others, so it pays to check this out *before* telling them about yourself.**

12. A "cookie" is a file that's sent to your Web browser by a Web site you've visited. Cookies are used on many commercial sites to track which pages visitors go to, and monitor their activities. Which of these statements about cookies is true?

    a. Cookies can track which other sites you visit after you leave a particular site, and even what ads you click on.
    b. Cookies can get data and personal information from the hard drive of your computer.
    c. Cookies can read your e-mail address.
    d. Computer viruses can be sent in cookies.

    a. **Yup, those little cookies are meant to track people, and the more information a cookie collects about where you surf, the more valuable it becomes! Marketers can even use cookies to keep track of what ads you click on, so they can send out banner ads – tailor-made just for you!**
    b. False. Cookies are only text files, so they can't "get" data from your computer hard drive or steal sensitive information about you. But you know what? Even without cookies, many sites you log on to can see lots of information, such as your service provider, your operating system, your browser type, your IP address, plug-ins you've downloaded, and even the kind of monitor you use!
    c. False. A cookie is only a piece of text. It's not a program or a plug-in, so viruses can't be sent through one.
    d. False. A cookie is a simple piece of "text" that lives on your hard drive once its been sent. Cookies alone can't "read" your e-mail address and send it back to a Web site. Cookies do become a problem, though, when they are used to collect information along with more aggressive software, such as Web bugs.

13. What makes the Internet so appealing to marketers?

    a. It's popular with kids and teens
    b. The spending power of kids is worth billions of dollars
    c. It's an interactive medium
    d. It's an effective tool for collecting personal information
    e. All of the above

    a. You're partly right! With thousands of kids using the Web at home and at school, marketers have decided that this is a pretty good place to grab your attention. Can you say "target market"?
    b. You're partly right! It's been estimated that by 2006, Canadian kids and teens will be spending over $1.8 billion dollars online annually. (Hey, maybe I should ask for a raise in allowance!)
    c. You're partly right! What the Internet does that TV can't, is actively involve kids in online games, contests and activities. Marketers know that while you're surfing, your brain goes into a kind of 'flow state' that makes you more receptive to messages. Normal commercials won't work online, because they interrupt the flow and are just plain annoying. Instead, marketers blend their ads with activities so kids won't notice they're being sold to. It's sneaky, but it works!
    d. You're partly right! Internet technology lets marketers gather all sorts of information through online surveys, quizzes and registration forms. They can even track where kids surf on a site, how long they stay, and what they download. Then they take this information and combine it to get a full understanding of their customers. This is called "data mining" – and thanks to the Internet, marketers have struck gold!
    e. **You got it! Marketers are flocking to the Internet because it's a popular place for kids – and kids have lots of money to spend. By getting kids to *interact* with activities and Web sites, marketers can sell you stuff and gather information without you even knowing it!**

14. What's the best way to tell whether it's safe to submit a credit card number to purchase something from a Web site?

   a. Find and click on the small padlock icon on your web browser.
   b. See if the site you're at provides you with clear information about its security practices.
   c. Look for "https:" in the Web page address.
   d. Check with your parents.
   e. All of the above

   a. A good start! Did you know that when you click on the padlock icon (which is also called a security icon) you can find out lots of information about the site you're on? – including whether or not the page is encrypted, so that other people can't look at your financial information.
   b. I'll only spend my hard-earned cash on sites that protect my privacy! Responsible sites tell you straight out what software they use to encrypt your credit card number so no one else can get it. Some sites will even give you an option to order by phone or mail.
   c. It pays to read the fine print in those Web addresses. If the beginning of the URL for a Web page says "https:", the "s" indicates that you're on a secure page, where it's safe to submit information.
   d. Smart kid! Checking with your parents before you buy anything online is a good idea. This goes for any stuff you plan to order. Whether you're paying for it over the Internet or being billed for it later, check it out with your folks first.
   e. **Right on! If you want to be sure that you're not tossing your hard-earned cash into cyberspace, make sure the site you're buying from is secure by clicking on the padlock icon in your Web browser; looking for the "https:" notation in the Web address; and checking out the encryption software that the site uses. And don't forget to check it out with your parents before you buy anything!**

15. The best way to handle junk e-mail is to hit the reply button and tell them not to send you any more spam.

   a. True
   b. False

   a. Uh-oh! When you reply to junk e-mail – even just to say not to bother you – you're letting the sender know that this is a working e-mail address, which means he'll continue to send you stuff. Instead, file junk mail to your trash folder or check out your e-mail options to see if you can block them altogether. If the e-mail is smutty or rude, forward the message to your e-mail service provider.
   b. **You got it! To say no to Spam – block it, put it in your trash file or forward it to your service provider. Don't send it back!**

16. You've found some interesting information on a Web site. What's a quick way to check whether it's legitimate?

   a. Go to a Web server like Alta Vista and run a search on the author's name.
   b. Go to a server like Alta Vista and type in **link:** followed by the site's address.
   c. Compare what you found on the Web site to other sources on the same topic.
   d. Check it out with a teacher, librarian or parent.
   e. All of the above

a. This is a good start. Remember that homework site I found that was really a hate site? When I did a search on Earnest Dumbell, I found his site listed on the HateWatch site and in connection to an article in *Macleans* magazine called "Hate Sites on the Web."

b. This is smart too. If you type in **link:** plus the full address of a Web site, you get to see the other sites that link to it. When I checked out "Homework Central," I found out that all sorts of hate sites linked to it, as well as a dozen organizations that monitor hate sites on the Web.

c. Sometimes it really pays to check out other sources. My friend found an essay on the Web that said if you got sunscreen in your eyes, it would make you blind. Luckily, she contacted Health Canada and found out it was just a rumour.

d. When you're not sure about information you've found on the Web, it really pays to check it out with your teacher or parents – **before** you start your project. (Why waste time if you don't have to?)

e. All these things can help you decide whether the information you're getting is the real stuff!

17. Which of the following can't spread computer viruses:

    a. E-mails
    b. Downloadable files from Web sites
    c. Text documents
    d. Disks or CDs

a. Oops! Sorry to break it to ya, but viruses can easily be spread by attaching themselves to e-mails. That's how the "ILOVEYOU" virus caused so much trouble: every time someone opened the infected attachment, the virus sent itself to everyone in that person's address book. That's why it's always important to tell people when you send e-mails with attachments – and to double-check with friends before opening anything they send you. Virus protection software is your best defence against these nasty bugs!

b. Not so. This is the best reason for NOT downloading pirated software from the Net – you may be getting lots more than you bargained for!

c. Correct. Text documents can't contain viruses because they aren't executable files. (That's why you don't have to worry about cookie files spreading viruses – they're text-based.)

d. Watch out when you're sharing CDs and disks with friends, 'cause you can't always tell right away if there's a virus lurking. Some viruses appear the minute you execute the code, while others are programmed to remain hidden until they're executed by your computer at a later date. Once again, it pays to have that virus protection software installed!

18. When you're surfing the Net, Web sites can find out information about you through:

    a. Your Internet Provider (which connects you to the Internet)
    b. Your computer name
    c. Cookies that are lodged on your hard-drive
    d. The last Web site you visited
    e. The plug-ins installed on your system
    f. All of the above

a. You're partly right. Your Internet Provider, or IP address, is one way that you can be traced on the Internet. An IP address is like a phone number for your computer, provided by the company that helps it connect to the Internet.

b. You're partly right. If your computer is part of a network (such as a school

computer), it will have a "host name" that identifies it. This information can be traced.

c. You're partly right. If you've visited a site before, and it has placed a cookie file on your hard drive, a profile of previous visits can be accessed by the Web site.

d. You're partly right. When you click on a link, the address of the page it's on will be sent to the new site you're linking to. This is called "referrer" information.

e. You're partly right. When you visit a Web site, your computer lets its server know what plug-ins (the software that lets you listen to audio, or play videos online) are on your computer.

f. **Correct! These are all ways that Web sites can find out stuff about you. Just by visiting a Web site, you give away lots of information to anyone who's interested – information about your computer, where you've been online, the colour of your socks (well, maybe not, but you get the picture).**

19. According to MNet, what percentage of Canadian teens in Grades 7-11 believe that all information on the Internet is true?

    a. 3%
    b. 6%
    c. 36%
    d. 48%

a. **This one's the right answer. Luckily, only 3% of teens believe that everything on the Net is true. They'd better be careful, 'cause there are all sorts of scam artists online who are just waiting for gullible kids like these.**

b. Six per cent of teens think that none of the information on the Internet is true. It's a good idea to be sceptical, but if you want my opinion, that's being a bit too paranoid!

c. Wrong-o. This is the thirty-six per cent of teens who think that most of the information they find online is true. (They also believe that most stories in the *National Enquirer* are true as well, but that's another story!)

d. Not this one. This is the percentage of smart teens who know that only some of the information on the Internet is true.

20. Most students in Grades 7-11 take steps to confirm that the information they find online is accurate or true.

    a. True
    b. **False**

a. Unfortunately, this answer's wrong. Less than three out of ten students take the time to double-check that the information they find online is accurate.

b. **You got it. A whopping 67% of students don't take any steps to confirm the accuracy of information they find on the Net. With all the hoax sites and misinformation out there, they'd be smart to double-check their facts before using online information for assignments – unless it's for a creative writing course.**

The *Jo Cool or Jo Fool* online scenarios were developed by MNet's Jane Tallim and Valerie Steeves. The *Jo Cool or Jo Fool* Teacher's Guide and Quiz were written by Jane Tallim.