



CHAPTER 5:

PROTECTING YOUR PRIVACY AND SECURITY ONLINE

Every time you go online, you face potential privacy and security problems. It should come as no surprise that computers are vulnerable to attacks by viruses, worms, Trojan horses and spyware. These are known as malware or pestware, because they're just plain bad (mal) or annoying (pest) software.

For many high school students, understanding computers often means just one thing: downloading music. Anyone with a computer and the right software can make digital copies of music from CDs, store these copies on their computer's hard drive and trade them with other users through the Internet. What most people don't realize is that when you use a file-sharing system like KaZaA, Grokster, Gnutella, Morpheus or LimeWire, not only can you share MP3 files, movies, software and anything else that can be exchanged across a digital network, but you are opening up your computer to all kinds of malware.

With file-sharing, every user's system acts as a server for everyone else's, so there is almost no way to control the flow of

information or what comes into your computer. As a result, by opening your computer to receive files from other computers, you are opening up your system to a hornet's nest of potential problems, including viruses, worms, Trojan horses, data theft and spyware, among other things.

Perhaps you want to know a bit more about these pests and how to prevent their destruction. Here's a brief explanation for each of these, followed by the best protections currently available. While this applies to others besides students and their use of computers, it is especially important for students' advisers to understand fully the privacy and security issues related to downloading on school-owned computers.

Some spyware hijacks you to other Web sites or changes the appearance of your Web browser.

Viruses and Worms

A virus is, in essence, a computer program that's usually hidden within another program or file. It tells your computer to do something that may be harmful, innocuous or even amusing. It's called a virus because it spreads like a cold, and no one wants to catch it. A computer virus is usually spread through e-mail attachments. You could be passing one from your computer to everyone you e-mail without even knowing it.

A worm is a particular type of virus, but it is more insidious than most. It can replicate itself and spread without any interaction on your part. A worm usually takes control of your computer, using up resources; it may even send itself to everyone in your e-mail program. It can also open access to your computer by others.

Trojan Horses and Spyware

Similar to the Trojan horse of Greek mythology, today's Trojan horse is any piece of software that appears useful and welcome but, once installed, sneaks other types of programs onto your computer. When you download music or computer programs, if the site states that it is supported by adware, there's a very good chance that it will install a Trojan horse on your system, along with the download you requested. One of the most common types of Trojan horse programs installed on computers is dialer programs, which use your computer and phone lines to make expensive phone calls without your knowledge.

Spyware is often loaded as a Trojan horse, but may also be loaded by one of your own

software vendors. A spyware program can surreptitiously monitor your computer usage and report your actions to others. You may have given permission to a site or a vendor to monitor your online usage "in order to provide better service to you," or you may have gotten the spyware without your knowledge. Some spyware hijacks you to other Web sites or changes the appearance of your Web browser. Some is referred to as "adware" because it uses information about the sites that you visit to customize ads to your computer. There are also spyware programs known as "keyloggers" because they log every key you press and then send the log to someone who may search the files for passwords, bank account numbers and so on.

Although you may not mind receiving ads in order to obtain free downloads, or may not object to the new look of your browser, you probably would feel differently if you found that someone had installed a keylogger on your system. Even the least harmful spyware—which simply places cookies on your computer—can slow down your system considerably, eating up resources and bandwidth. If you're determined to download freebies off the Internet or to share files (music, movies, etc.) with others, be sure to disable file sharing on all other files, so that no one can read files from your system. Many computer applications often run in the background of your computer when you think you've actually shut them down. Look for a way to disable the file sharing altogether.

Another option is to create a specific directory to be shared and copy all the files you want to share into that directory. Make that the only directory you share and don't

enable sharing for any other directories or subdirectories.

Another simple and more thorough work-around is to run a separate computer that is only used for these downloads. If anything that you've downloaded is destructive, you can reboot the computer from the original startup CDs that came with the computer and reload everything, if necessary. So long as you don't do anything else on this computer, or store anything of interest, you're reasonably safe in downloading.

Other Potential Risks to Privacy

POP UPS

Pop-ups are ads that “pop up” in a separate page when you're trying to view a Web site. Since advertising supports some of what is available to us on the Web, users may simply have to get used to seeing these pop-ups. Most of these are just a nuisance, getting in the way of what you're trying to see. However, some are worse, downloading spyware to your system when you click on them. For protection against pop-ups, see Pop-Up Stoppers below.

COOKIES

A cookie is a file that is placed on your computer when you visit a Web site. It usually contains some type of identifying information such as a number assigned to you, in order to identify you and welcome you back for return visits. It also can contain your name, address and anything else that you care to fill out on the Web site. A classic example of how this information might be useful is a news site

that allows you to customize what you want to see on the front page of your news. If you fill out your preferences (i.e., selecting national news, sports, entertainment, your local weather, based on the zip code you enter), the Web site places this information into a cookie, stores it on your computer, and retrieves it when you return to that site, in order to give you your own personalized news page. If cookies stopped there, they would not be of much threat to your privacy. But of course, they don't stop there.

There are search engines that save the terms that you've searched on in order to guess at your interests and market to you. Frankly, they don't do this very well. If you've researched the company Naked Food-Juice or the radio show Naked Scientists, you've very likely been identified as a pornography consumer, even if you've never visited a porn Web site. There are some unsavory consequences to this kind of misunderstanding, which will be explained in the next section.

There are also companies that cooperate in sharing the information you've filled out, terms you've searched, and Web sites you've visited, in order to develop a more comprehensive profile of your interests. In this case, even sites you've never visited may recognize you on your first visit. Companies that gather information about your Web usage are usually interested in selling you something. If you don't fill out any information on Web sites, they may only be able to send you pop-up ads; however, the more information you provide, and the more that they share with their partners, the more likely that they'll also obtain your e-mail address and start deluging you with spam (junk e-mail).

Pop-ups are ads that “pop up” in a separate page when you're trying to view a Web site.

Every time you send your e-mail address to a company or Web site, you've increased the odds that it will make its way to a marketing database.

To stop Web sites from recognizing you, delete the cookies that are already on your system, use a firewall or other security software to stop cookies from bad sites, and make it a practice to remove your cookies periodically. Be aware that stopping cookies will stop you from accessing some Web sites, and deleting cookies will delete any preferences that you've set on the sites that you visit. See Cookie Crumblers below for additional information.

SPAM (JUNK E-MAIL) OR UCE (UNSOLICITED COMMERCIAL E-MAIL)

If you're a spam fan, you're in luck: There's no way to get rid of it! If you'd like to receive an e-mail box chock full of ads, all you have to do is perform some online searches, and fill out your e-mail address on a few Web sites.

Worse than junk mail, if a search engine has erroneously identified you as a consumer of porn, your spam can come in the form of extremely graphic and shocking pornography, which can even go to children. You can't opt out. You can't even tell marketers, "No thanks, I'm not interested in your porn, but could you send me ads for educational products?" In fact, if you click on a link to remove your e-mail address, you have confirmed that it is a good address, and it is more likely to be resold, increasing your spam. Going to the Web site of a marketer to fill out their opt-out form can even result in you receiving more spam or in spyware being loaded on your computer. The Federal Trade Commission has been trying to tackle the spam problem for a while, as has the legislature of every state. None of these efforts has been successful.

Until they are, you can take steps to slow marketers from getting your e-mail address:

- Don't give out your e-mail address. Every time you fill it out on a Web site, or send an e-mail to a company or Web site, you've increased the odds that it will make its way to a marketing database.
- If you must give a company or Web site your e-mail address, read their privacy policy first, and be sure to check off any boxes that allow you to "opt-out" of marketing.
- Don't ever place an e-mail address link on a Web page that you create, including that of your school. There are automated tools (bots and spiders) that crawl across Web sites to harvest this type of information for resale. In fact, according to research conducted by the Center for Democracy & Technology, e-mail addresses posted on Web sites attract the most spam.
- If you must place an e-mail address for a contact on a Web site, try one of the following methods to confuse the bots and spiders:
 - Replace characters in an e-mail address with human readable equivalents (e.g., person@company.com) would be changed to "person at company dot com").
 - Insert e-mail addresses onto your Web page as pictures or word art, rather than text or links.
- Understand that these methods may only work for a short time until more sophisticated bots can be programmed to work around these strategies. Never respond to spam.
- Don't use your "good" e-mail address for Web site questionnaires. Try one of the following instead:
 - Use a disposable e-mail address. Many

companies (such as Hotmail and Yahoo) will give you free e-mail accounts that you can change as soon as you start receiving spam on them. Your ISP may also provide extra e-mail addresses that you're not currently using that you can create, use and delete at will. There are even companies (such as SpamGourmet, E-mailias, Mailshell and Spamex) that provide temporary e-mail addresses that expire at a certain point, or after a certain number of messages.

- Try to make your e-mail messages anonymous, using an Anonymous Re-mailer, as explained below.
- NEVER, NEVER, NEVER buy anything from a spammer! If spamming didn't sell products and services, spammers wouldn't use it.

See Spam Filters below for additional tactics for dealing with spam.

CHAT, AIM, INSTANT MESSAGING AND NEWSGROUPS

Chat is not private. Neither are newsgroups. When you chat online, you never know who is eavesdropping. There are people who misrepresent their age, gender or other important factors in order to gain your confidence. Adults can become victims, but students are especially vulnerable to online predators.

Twenty-four percent of 550 American teens surveyed by Harris Interactive in 2003 said they had been contacted online by a stranger who tried to arrange an off-line meeting. Microsoft's MSN service shut down its chat rooms in 28 countries partly due to concerns about sexual predators preying on minors. But those numbers continue to grow.

In addition to predators, spammers use chat rooms to collect e-mail addresses in order to add them to databases for resale.

If you participate in online chat or newsgroups, there are some basic rules meant to keep you safe and outwit spammers:

- Never give out personal information, including the name of your school, your real name, your photograph, your home town or any other identifying information.
- Don't use your "good" e-mail address for newsgroups. Try one of the companies listed above for a disposable e-mail address.
- Make your newsgroup messages anonymous, using an Anonymous Re-mailer, as explained below.
- Never plan a face-to-face meeting with anyone you meet online. If you plan to meet someone, take an adult with you or talk with your parents first.

A WARNING ON NEWSGROUPS AND CHAT ROOMS

For the sake of a news story, you should never quote anyone you met in a newsgroup or chat room. Any information that you gain there should be verified elsewhere. Chat room and newsgroup information should be treated as gossip, and be given just as much credence.

When it comes to online privacy, you can be your own worst enemy. It starts with who has access to your computer. If computers are shared among many users,

Chat is not private.

Neither are newsgroups.

When you chat online, you never

know who is eavesdropping.

The best protection against computer viruses and worms is a good virus protection package.

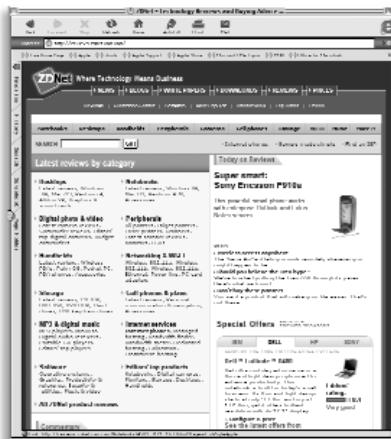
as they are in school, are they secured so that they can't be removed or stolen? Are they password-protected so that the data on them is protected, and so that no one can send inflammatory or illegal messages from them?

What about those passwords? Do all of the users of the computers have unique, less-than-obvious passwords that are kept private (*never* shared with friends) and changed periodically?

If the computers are physically secure and passwords are handled responsibly, there is still the need to educate all computer users about the need to keep personal information private. Privacy software can't save you from yourself: If you're sharing your password, or placing your e-mail address, name, home address or other private information online, you are your own worst enemy when it comes to online privacy. Before purchasing a privacy software package, look at the more fundamental ways that personal information is gathered and make sure that appropriate policies and practices are put into effect and honored. Online privacy problems are as much people problems as they are computer problems.

Privacy Protection

There are many wonderful and some not-so-wonderful privacy and online security packages available, both over the Internet (sometimes for free) and in the stores. They are not all alike, and some can cause



additional problems on your system. A program that is effective today can be out-of-date tomorrow, when new privacy threats are discovered.

Rather than recommending a specific program, a more prudent approach would be to read current reviews by industry experts and

actual users. Before using a free version or purchasing a full version of any software package, see a review site like ZDNet (select *Security & Utilities* under *Software* at reviews-zdnet.com.com), or PC Magazine (select *Reviews* at www.pcmag.com) to find out if there are any problems with the software you plan to purchase or download, whether it will do all that you hope and is easy to use.

VIRUS PROTECTION SOFTWARE

The best protection against computer viruses and worms is a good virus protection package such as Norton AntiVirus or McAfee VirusScan. Your Internet Service Provider or school may run your e-mails through a similar package for you automatically. If not, you absolutely should have a virus protection package on every computer that you send or receive e-mail on, and should be sure to update it frequently so that you'll have protection from newer viruses as well. If your virus software is not updated, your computer will be vulnerable to each new virus that emerges.

Macintosh computer users have had greater protection from the threat of viruses, but they should not become blasé about this

threat. Virus protection software is a good idea for *all* computers.

ANTI-SPYWARE PROGRAMS

Many sites offer to scan your system for spyware for free. They are not all the same. Some will scan your system and notify you of the spyware, but will not remove it, while others will do both. Many will install their software onto your system in the process, which can be very difficult to remove. All are hoping that you will buy the full version of their software.

You will find that each anti-spyware program catches a different set of spyware programs, and it's probably worth running more than one on your computers to remove every detectable piece of spyware. At that point, you'll want a firewall to stop newer spyware from getting into your computer, as spyware producers keep getting more imaginative and ingenious at thwarting the firewalls. You'll also need to download updates or run newer versions of anti-spyware programs periodically to catch what your firewall misses.

POP-UP STOPPERS

The best way to avoid annoying or even malignant pop-ups is to use a pop-up stopper/blocker program. There are many available, and some are free. Google, Yahoo, MSN and others offer one with their free toolbar, and some ISPs do as well. Most of these do work pretty well but, as always, read the reviews before downloading or purchasing software. It is important for you to read the reviews and get the latest, greatest pop-up stopper, as the tools change often and all of them can change their mission at any point.

COOKIE CRUMBLERS

There are software packages specifically designed to remove cookies from your system. You can also do this yourself. Instructions for removing cookies can usually be found on your browser's support Web site. Further information about deleting cookies and stopping them from coming back can be found from Junkbusters (www.junkbusters.com/cookies.html) and TinHat.com (www.tinhat.com/internet_cookies/index.html). Some other types of privacy software, such as firewall software, often include cookie removers, so before you purchase one, make sure you don't already have a cookie remover within another privacy package.

SPAM FILTERS

Spam filters can stop you from receiving some junk mail. Your e-mail software may perform this function, with settings or options that you can select to screen out some spam. The risk is that a spam filter that catches all spam can also reject messages from your friends, family and associates, so you should understand the options before setting them.

Your Internet Service Provider may also perform this service for you, or you can purchase one of several spam filtering packages available on the market. The main problem with these packages is that spam creators learn what the packages do to identify spam, and then change their e-mail messages to outsmart them. It's definitely a cat-and-mouse game at this point. If you purchase a spam filter, make sure it's the most current version and download updates often to stay one jump ahead.

**Spam filters
can stop you
from receiving
some junk
mail.**

A firewall is software that places a barrier between your computer and the Internet (or smaller computer networks).

Some spam filters let you keep your spam e-mails in a “holding pen,” which allows you to view them and approve messages from senders you recognize.

ANONYMOUS RE-MAILERS

An anonymous re-mailer receives e-mails from you, strips off your identifying information and re-mails it to the destination of your choice. Most of these services charge a monthly or yearly fee, but there are still some free re-mailers as well. For more details on how they work, see this page from About.com e-mail.about.com/library/weekly/aa031300a.htm

While students may not use these, some investigative reporters use anonymous re-mailers to work on undercover investigation projects without revealing too much information about their employers. Still, it is worth everyone knowing about them.

FIREWALLS

A firewall is software that places a barrier between your computer and the Internet (or smaller computer networks). It stops unwanted programs from being installed on your computer and stops others from accessing your computer without your knowledge. Ideally, it also stops your computer from sending information to others without your permission.

You can purchase a firewall or download one, or your ISP may provide one. Each company makes different claims about what their products does, as “firewall” has become a generic term, and has been interpreted by many software developers to mean different things. In order to compete with all of the other firewall software, the

company may also include a cookie crumbler, anti-spyware program or other software meant to provide additional protection or make the product easier to use.

Spyware developers and virus creators are very interested in and knowledgeable about firewalls, as they continue to build software capable of bypassing as many firewalls as possible. For this reason, it’s important that your firewalls are updated regularly, and that you continue to scan your system for viruses and spyware, even after installing a firewall.

INTERNET FILTERS

There are several types of Internet filtering. Filtering of search results is provided by some of the search engines. For example, Google offers two levels of “Safe Search Filtering” on its preferences screen (www.google.com/preferences), Yahoo provides two levels in its “Safe Search Filter” (search.yahoo.com/search/preferences?pref_done=http%3A%2F%2Fwww.yahoo.com&fr=fp-top), and AltaVista offers a “Family Filter” (www.altavista.com/web/ffset?ref=Lw).

There are Web guides or directories such as Yahoooligans (yahooligans.yahoo.com) and Cool Safe Links for Kids, Parents and Teachers (www.karscot.com/kidlinks.html), providing safe content for kids.

There are also Internet filtering software packages available for purchase. Most of these come in the form of Parental Control software, which include Internet filtering and online usage monitoring, and may also screen e-mail. These packages are created to keep kids safe online, but they are no substitute for parental supervision.

Some schools and companies have created a subset of the Internet, providing only sites that have been filtered and deemed safe. Sites like The Children’s Internet (www.childrensinternet.com/home.html), MSN Kidz (kids.msn.com) and Earthlink Kids Channel (kids.earthlink.net) all provide kid-oriented content, parental controls and filtering capability for their users.

If your school has Internet filters for the students, or if students use the filtered versions of search engines, be aware that these can skew their research. For example, if a student is researching *breast cancer*, sites containing the word *breast* may be filtered out due to obscenity filtering. Similarly, if they look for news about the 2004 Superbowl, many sites and stories might be filtered out because of the Janet Jackson “clothing malfunction,” in which she revealed her breast on national television. This type of filtering can affect any journalist’s ability to see the big picture and do his work, and illustrates why journalists of all ages need sources other than the Internet for their research.

ONLINE MONITORING SOFTWARE

Online monitoring software is sold in a few forms. One popular type is meant to allow parents to monitor their children’s online usage and keep them safe, as noted above. Another type is marketed to spouses wishing to surreptitiously check on their mates. Another type is for employers who wish to make sure that their employees aren’t wasting time on the Internet, or sending out company secrets via their e-mail. There are also keyloggers, which keep a file of every transaction you make in order to follow in your online footsteps and find out where you have been. Any of these can also be used by an individual

wishing to see if anyone else has used his or her computer. So you see, online monitoring systems can be used to invade someone else’s privacy or to secure your own. While this may not be important for students at school, students should be aware that their every online move may be monitored at home if parents are concerned about their online activities.

SYSTEM BACKUP AND ROLLBACK PROGRAMS

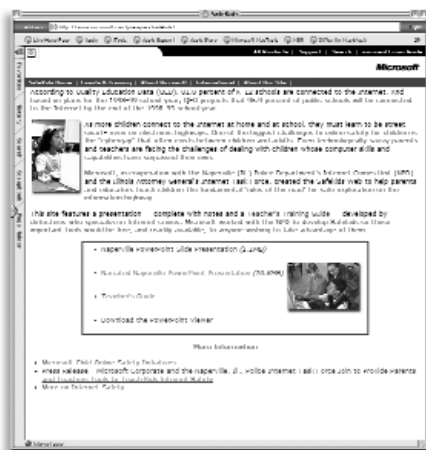
You can and should manually back up all of the critical data on your system on a regular basis. There are programs that can automate this process for you.

Rollback programs take it a step further, saving copies of your system and reverting back your whole computer to a previous point of your choosing when problems are experienced. It can be difficult to decide when to revert to, as it’s not usually clear when a virus or piece of spyware was loaded to your system. Each can sit dormant for some time before causing trouble and making itself apparent. That’s why it’s useful to have many backups from which to choose in case malware re-emerges and you need to move to an earlier version of your system.

INTERNET OR ONLINE SECURITY PACKAGES

Internet security programs, online security packages—these terms can apply to any of the privacy software covered to this point, or any combination of it. There is no single package that does it all (although some claim to), but a true online security package should cover as many of the types of threats and protection as possible. When comparing online security packages, you’ll

You can and should manually back up all of the critical data on your system on a regular basis.



be comparing apples and oranges, as they all offer various types of protection from assorted collections of threats. Even if two programs are designed to protect you from spyware and viruses, they don't protect you from the same spyware and viruses, or accomplish this with equal success.

and procedures that are not only in place but taught to every student and teacher who accesses the Internet.

If you don't have such policies and procedures in place at your school, check with the people in charge of technology at the school. If they are not equipped to help, check with your school district or board of education. If you don't find that the online safety issues have been sufficiently addressed at your school, you can find additional help from organizations such as i-SAFE America (www.isafe.org), a nonprofit organization whose mission it is "to educate and empower youth to safely and responsibly take control of their Internet experiences." Another excellent site is SafeKids (www.microsoft.com/presspass/safekids/), created by Microsoft, in cooperation with the Naperville (IL) Police Department's Internet Crimes Unit and the Illinois Attorney General's Internet Task Force, and intended "to help parents and educators teach children the fundamental 'rules of the road' for safe exploration on the information highway."

Although the Internet is an indispensable educational and communication tool, and has become an integral part of virtually every newsroom, there are dangers online, particularly to children and teens. It's important that the adults in charge take a proactive approach to providing both a safe online environment and the education to handle online usage safely and responsibly. This is the responsibility of every teacher who sends a student to the Internet for information. Fortunately, teachers and organizations around the world are willing and able to help you accomplish this. ■

Although the Internet is an indispensable educational and communication tool, and has become an integral part of virtually every newsroom, there are dangers online, particularly to children and teens.

It's up to you to decide which protections are essential to you, and what the best value is. This can be very complicated, as some of the free packages are excellent and you won't need to make a purchase, and you probably already own some of the pieces of your privacy and security picture. Some packages may also offer capabilities that you don't really want or need.

After assessing your privacy and security needs, and determining which can be met with your existing software, read current industry reviews of all of the software packages that you're considering, along with user opinions. Providing these resources is some of what the Internet does best, and will help you to make informed and wise decisions to keep students safe. Your school system may provide online security packages and some may not allow you to provide your own. Be sure to check your school's policies.

The Journalism Teacher's Responsibility

In addition to privacy software, every school that teaches students to access the Internet should have privacy and security policies